(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 502 442**

(51) Int. CI.:

G01R 31/317 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.01.2011 E 11700335 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.06.2014 EP 2526433**

(54) Título: **Circuito integrado de silicio que incluye una función físicamente no reproducible, procedimiento y sistema de test de dicho circuito**

(30) Prioridad:

18.01.2010 FR 1050297

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.10.2014

(73) Titular/es:

INSTITUT TELECOM - TELECOM PARIS TECH (100.0%)
46, Rue Barrault
75013 Paris, FR

(72) Inventor/es:

DANGER, JEAN-LUC

(74) Agente/Representante:

RIZZO, Sergio

DESCRIPCIÓN

Circuito integrado de silicio que incluye una función físicamente no reproducible, procedimiento y sistema de test de dicho circuito

[0001] La invención hace referencia a un circuito integrado de silicio que incluye una función físicamente no reproducible y un procedimiento de selección mediante un test de fiabilidad de dicho circuito. Se aplica, especialmente, en el campo de los circuitos de criptografía y autentificación de componentes electrónicos.

[0002] Para numerosas aplicaciones, resulta útil poder identificar de manera precisa un chip electrónico o un circuito integrado. En la técnica anterior se propusieron soluciones que permiten, especialmente, distinguir un circuito dado de entre una serie de circuitos procedentes de la misma cadena de producción. De este modo, incorporar en un circuito integrado una función físicamente no reproducible de tipo PUF, acrónimo procedente de la expresión anglosajona “Physically Unclonable Function”, permite la generación de una firma única propia a dicho circuito. Esta firma puede ser utilizada con el fin de poner en marcha un mecanismo de autentificación de sistema electrónico.

[0003] Esta firma única puede igualmente ser utilizada como clave de cifrado única propia al circuito. En este caso, no se requiere la memorización de la clave dentro del circuito integrado.

[0004] Las firmas son generadas directamente por los circuitos. Al no ser requerida la intervención humana, se ha visto mejorada la resistencia a ataques, especialmente ataques tales como la observación.

[0005] En el estado de la técnica existen diferentes maneras de aplicar funciones PUF. Así, el artículo de R. Pappu titulado Physical One-Way Functions, PhD Thesis, Massachussetts Institute of Technology, Marzo 2001, describe qué es una PUF óptica. Las PUF ópticas están compuestas de un material transparente que contiene partículas dispersadas aleatoriamente permitiendo la desviación de la luz láser.

[0006] Las PUF peliculares, designadas por la expresión anglosajona “coating PUF”, son igualmente utilizadas. Este tipo de PUF viene descrito en el artículo de P. Tuyls, B. Skoric y T. Kevenaar titulado Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting, Secaucus, NJ USA: Springer-Verlag New York, 2007. En este caso, un material opaco es estimulado aleatoriamente con partículas dieléctricas y posicionado por encima del circuito integrado.

[0007] Una familia de PUF denominadas PUF de silicio utiliza las incoherencias estructurales introducidas por los procedimientos de fabricación de los circuitos integrados. La diferencia de dispersión entre los hilos y los transistores que constituyen dichos circuitos es en efecto significativa de un circuito a otro, aun formando parte del mismo grupo. Esa familia comprende, especialmente, las PUF árbitros, las PUF de oscilador en anillo y las SRAM PUF. Las PUF de silicio pueden aplicarse en circuitos ASIC o FPGA sin ninguna modificación tecnológica.

[0008] Las PUF árbitros vienen descritas en el artículo de B. Gassend, D. E. Clarke, M. van Dijk, y S. Devadas, titulado Silicon physical random functions, ACM Conference on Computer and Communications Security, 2002, páginas 148-160. En este tipo de PUF, una misma señal se propaga tomando dos caminos de un circuito de retardo, siendo los dos circuitos distintos y pudiendo ser configurados con la ayuda de palabras de control. Un árbitro compara el retardo entre las dos señales que resultan de estas dos propagaciones, y el resultado de esta comparación desemboca en la firma del circuito integrado. Uno de los inconvenientes de este tipo de PUF es que los elementos que permiten la parametrización de los caminos deben estar equilibrados en términos de retardos, lo que implica una dificultad a la hora de su diseño.

[0009] Las PUF de pares de osciladores en anillo son también PUF de silicio. Aparecen descritas en el artículo de G. E. Suh y S. Devadas titulado Physical unclonable functions for device authentication and secret key generation, DAC, 2007, páginas 9-14. Aquí se comparan las frecuencias generadas por un par de osciladores en anillo idénticos. El resultado de esta comparación desemboca en la firma del circuito integrado. Un inconveniente de los osciladores en anillo es que dichos osciladores son sensibles a los efectos denominados de segundo orden como, por ejemplo, los efectos vinculados al acoplamiento mutuo entre los osciladores o las perturbaciones introducidas en un oscilador en el momento de un ataque.

[0010] Un objeto de la invención es, especialmente, paliar los inconvenientes descritos anteriormente.

[0011] A tal fin, la invención tiene como objeto un circuito integrado de silicio que incluye una función físicamente no reproducible LPUF que permite la generación de una firma propia a dicho circuito. Dicha función incluye un oscilador en anillo compuesto por un bucle recorrido por una señal e, estando formado dicho bucle por N cadenas de retardo topológicamente idénticas, conectadas en serie entre ellas, y una compuerta de inversión, estando compuesta una cadena de retardo por M elementos de retardo conectados en serie entre ellos.

Asimismo, incluye un módulo de control que genera N palabras de control, estando utilizadas dichas palabras para configurar el valor de los retardos introducidos por las cadenas de retardo en la señal e que les recorre. Incluye igualmente un módulo de medición que mide la frecuencia de la señal a la salida de la última cadena de retardo tras la actualización de las palabras de control. Asimismo, incluye medios para deducir de las medidas de frecuencia los bits que componen la firma del circuito.

[0012] El circuito es, por ejemplo, un circuito ASIC o un FPGA.

[0013] Según un modo de realización, la firma es utilizada como clave de cifrado.

[0014] Según otro modo de realización, la firma es utilizada para su autentificación.

[0015] Los elementos de retardo incluyen, por ejemplo, medios para bifurcar la señal que les recorre según al menos dos caminos distintos, introduciendo un camino un valor de retardo que le es propio, estando controlada esta separación por al menos un bit que pertenece a una palabra de control.

[0016] Según un aspecto de la invención, se presentan palabras de desafío compuestas por una concatenación de palabras de control a la entrada del módulo de control, generando dicho módulo combinaciones a partir de dichas palabras con el fin de configurar las cadenas de retardo.

[0017] Los bits de la firma se determinan, por ejemplo, en función de la clase de las frecuencias medidas por las diferentes combinaciones de palabras de control.

[0018] Los bits de la firma se determinan, por ejemplo, en función de las diferencias estimadas entre dos valores de frecuencia medidos, correspondiendo un valor de frecuencia medido a una combinación de palabras de control.

[0019] Los bits de la firma se determinan, por ejemplo, en función del valor de la relación entre dos diferencias de frecuencia estimadas.

[0020] En un modo de realización, el circuito incluye un generador de números aleatorios, siendo utilizados los números aleatorios con el fin de seleccionar el orden en el que son medidas las frecuencias correspondientes a las combinaciones de las palabras de control.

[0021] El circuito contiene, por ejemplo, al menos un bit de paridad, siendo utilizado dicho bit para corregir un bit de la firma generada con un error.

[0022] La invención tiene igualmente como objeto un procedimiento de test de circuitos integrados que contiene una función físicamente no reproducible LPUF. Se aplica una sucesión de etapas a los circuitos testados de modo que se seleccionen los circuitos que permiten generar una firma propia a dicho circuito con un nivel de fiabilidad elegido, correspondiendo dichas etapas a una selección de los parámetros T y Th de configuración del test, así como de B combinaciones de palabras de control con una distancia de Hamming al menos igual a un valor predefinido HD, y seguidamente a una fase de mediciones durante la cual se miden cantidades representativas de los bit de firma del circuito, realizándose hasta T mediciones por bit de firma, estando acumuladas esas T mediciones de modo que se decida si el bit correspondiente es indeterminado, habiendo tomado la decisión tras la comparación con al menos un valor deducido del valor del parámetro Th, estando seleccionados los circuitos testados en función del número de bits indeterminados detectados.

[0023] Según un modo de aplicación, el procedimiento incluye una etapa de determinación de la probabilidad para que un circuito no sea seleccionado, estando determinada dicha probabilidad utilizando la expresión:

$$P_{rej} = 1 - \left[1 - \mathrm{erf}\left(\frac{Th}{\sigma \times \sqrt{2 \times HD}} \right) \right]^{B}$$

en la que:

erf() es la función de error de Gauss;
σ es la varianza de las mediciones de las cantidades representativas de los bits de firma del circuito.

[0024] Según otro modo de aplicación, el procedimiento incluye una etapa de determinación de la probabilidad de error por bit de firma, estando determinada dicha probabilidad utilizando la expresión:

$$P_{e,j} = \frac{1}{2}\left(1 - erf\left(\frac{\sqrt{T} \times \delta_j}{s\sqrt{2}}\right)\right)$$

en la que:

δ_j es una diferencia de frecuencia medida entre dos frecuencias que corresponden a la aplicación de dos combinaciones de palabras de control distintas;
s, definida como s^2, es la varianza del ruido de medición.

[0025] Un circuito es seleccionado, por ejemplo, si ningún bit de la firma es indeterminado.

[0026] Cuando la función LPUF de un circuito testado está asociada a un bit de paridad cuyo valor está determinado a partir de la firma de dicho circuito, dicho circuito es seleccionado, por ejemplo, si el número de bit indeterminado es estrictamente inferior a 2.

[0027] Los valores de s^2 y σ^2 son medidos, por ejemplo, para una temperatura sensiblemente igual a +70Cº y una tensión de alimentación de los circuitos sensiblemente inferior al 5% con respecto a la tensión de alimentación nominal, estando efectuada la fase de mediciones en las mismas condiciones.

[0028] La invención tiene igualmente como objeto un sistema de test que aplica el procedimiento según la invención. El sistema está compuesto por un ordenador provisto de una interfaz de usuario, un equipo que permite controlar las sondas de medición, teniendo dichas sondas la función de recopilar las mediciones de las cantidades representativas de los bits de firma producidas por los circuitos testados, estando a continuación efectuados por el ordenador los tratamientos asociados a esta fase y mostrados en su interfaz.

[0029] Otras características y ventajas de la invención aparecen en la siguiente descripción que hace referencia a los dibujos adjuntos, que se muestran únicamente a título de ejemplo sin carácter limitativo alguno:

- la figura 1 muestra un ejemplo de una PUF árbitro;
- la figura 2 presenta un elemento de retardo que puede ser utilizado en una PUF árbitro;
- la figura 3 muestra un ejemplo de una PUF de silicio según la invención que contiene una estructura en bucle;
- la figura 4 muestra un ejemplo de elementos de retardo que pueden ser utilizados en una cadena de retardo comprendida en una LPUF;
- la figura 5 presenta una LPUF que comprende N = 2 cadenas de retardo;
- la figura 6 muestra un ejemplo de método de combinación de las palabras de control utilizadas en una LPUF;
- la figura 7 muestra un ejemplo de función de error que permite estimar la fiabilidad de las LPUF;
- la figura 8 ilustra el principio de la detección de bits defectuosos en una LPUF;
- la figura 9 muestra un ejemplo de combinaciones de palabras de control y comparación de las medidas de frecuencia asociadas que permiten reducir el índice de rechazo de un circuito que contiene una LPUF;
- la figura 10 muestra un ejemplo del procedimiento de test de circuitos según la invención;
- la figura 11 muestra un ejemplo de sistema de test que aplica el procedimiento de test según la invención.

[0030] La figura 1 muestra un ejemplo de PUF árbitro. Una PUF árbitro está compuesta generalmente por una cadena de K elementos de retardo 100, 101, 102 conectados en serie entre ellos, y un elemento árbitro 103 conectado al último elemento de retardo de dicha cadena. Se introduce una señal e en la PUF y recorre dos caminos electrónicos diferentes 104, 105. Los elementos de retardo 100, 101, 102 pueden estar configurados con la ayuda de una palabra binaria de control de K bits C_1, C_2, ..., C_K. A una palabra de K bits le corresponde una configuración para cada uno de los dos caminos 104, 105. Esta configuración es única para una palabra binaria de control dada, estando utilizado cada uno de los bits de dicha palabra para configurar uno de los elementos de retardo 100, 101, 102, poseyendo un elemento de retardo una función de separación y participando en la definición de los dos caminos únicos asociados a una palabra de control.

[0031] El elemento árbitro 103 compara los retardos introducidos por estos dos caminos 104, 105 entre las dos señales procedentes de e, desembocando el resultado de esta comparación en un bit Q. Modificando la palabra de control, se genera otro bit Q. De este modo, es posible generar palabras binarias utilizadas como firma del circuito en el que se aplica la PUF árbitro.

[0032] La figura 2 presenta un elemento de retardo que puede ser utilizado con una PUF árbitro. Este elemento de retardo es, por ejemplo, el elemento j de una cadena de K elementos. A la entrada de este elemento de retardo, se presentan dos señales $e_{0,j}$ y $e_{1,j}$. La salida de dicho elemento corresponde a dos señales s_0 y s_1.

[0033] Las señales de entrada son bifurcadas en función del valor que adopta el bit de control C_j, controlando dicho bit dos puertas 205, 206 que permiten dicha separación.

[0034] Por ejemplo, la señal $e_{0,j}$ puede tomar, bien un primer camino 200 si $C_j = 0$, o bien un segundo camino 201 si $C_j = 1$. En el primer caso, la señal de salida s0 corresponde a la señal de entrada $e_{0,j}$ afectada por el retardo d_o^j asociado al primer camino 200 y en el segundo caso, la señal de salida s1 corresponde a la señal de entrada $e_{0,j}$ afectada por el retardo d_1^j asociado al segundo camino 201.

[0035] En lo que respecta a la señal $e_{1,j}$, esta tomará entonces, bien un primer camino 202 si $C_j = 0$, o bien un segundo camino 203 si $C_j = 1$. En el primer caso, la señal de salida s1 corresponde a la señal de entrada $e_{1,j}$ afectada por el retardo d_o^j asociado al primer camino 202 y en el segundo caso, la señal de salida s1 corresponde a la señal de entrada $e_{1,j}$ afectada por el retardo d_1^j asociado al segundo camino 203.

[0036] Para que estos elementos de retardo permitan la aplicación de una PUF árbitro, es necesario que los caminos internos a dichos elementos de retardo estén equilibrados, es decir, que los caminos paralelos (200, 202) sean idénticos y los caminos cruzados (201, 203) sean idénticos. Este equilibrado es más complejo considerando que los caminos pueden cruzarse a nivel de cada elemento de retardo resultando, pues, compleja la aplicación de una PUF árbitro.

[0037] La figura 3 muestra un ejemplo de una PUF de silicio según la invención que contiene una estructura en bucle. La PUF de silicio de este ejemplo viene designada más adelante en la descripción por el acrónimo LPUF procedente de la expresión anglosajona “Loop Physically Unclonable Function”.

[0038] Una LPUF es una PUF de silicio que contiene un bucle 300 formado de N cadenas de retardo 301, 302, siendo N al menos igual a 2. Este bucle forma un oscilador en anillo simple.

[0039] Una cadena de retardo 301, 302 está compuesta por M elementos de retardo 303. A diferencia de una PUF de oscilador en anillo, el oscilador de la LPUF contiene un único oscilador.

[0040] Una de las ventajas de la estructura de una LPUF es que el ruido es común a todas las cadenas de retardo. Además, no existe problema de acoplamiento mutuo entre osciladores, ya que hay un único bucle.

[0041] Cada cadena de retardo 301, 302 recibe una palabra de control Ci de M bits, correspondiendo una palabra a un valor de retardo propio al circuito.

[0042] Un bit $C_{i,j}$ de una palabra de control C_i corresponde a un valor de retardo del elemento de retardo número j entre los M elementos de la cadena de retardo i.

[0043] A la hora de diseñar una LPUF y, más especialmente, a la hora de realizar la situación-encaminamiento que consiste en transformar las puertas lógicas y sus interconexiones en puertas con transistores y en hilos reales, la cadena de retardo es duplicada N veces de una forma rigurosamente idéntica. Cada duplicación puede ser aplicada fácilmente, tanto en el marco del diseño de circuitos ASIC como de circuitos FPGA. Por tanto, se desprende que una LPUF es especialmente sencilla de diseñar.

[0044] La figura 4 muestra un ejemplo de elementos de retardo que pueden ser utilizados en una cadena de retardo comprendida en una LPUF.

[0045] Una señal de entrada $e_{i,j}$ es introducida en el elemento de retardo 405. Dicha señal puede propagarse tomando dos caminos distintos 403, 404. La elección del camino depende del valor del bit de control $C_{i,j}$ asociado al elemento de control, teniendo dicho bit como objeto seleccionar uno de los dos caminos 403 o 404 con la ayuda de un multiplexor 400. Los índices i y j indican respectivamente el índice de cadena y el índice de elemento en la cadena.

[0046] A título de ejemplo, si $C_{i,j} = 0$, la señal de entrada $e_{i,j}$ tomará un primer camino 403 y la salida del primer elemento de retardo corresponderá a la señal $e_{i,j}$ afectada por un retardo $d_{i,j}^0$, resultando dicho retardo de la propagación de la señal a lo largo de este primer camino. Por el contrario, si $C_{i,j} = 1$, la señal de entrada $e_{i,j}$ tomará un segundo camino 404 y la salida del primer elemento de retardo corresponderá a la señal $e_{i,j}$ afectada por un retardo $d_{i,j}^1$, resultando dicho retardo de la propagación de la señal a lo largo de este segundo camino.

[0047] Ventajosamente, no resulta necesario realizar un equilibrado entre los diferentes caminos de un elemento de retardo 403, 404 ya que basta con duplicar los elementos de retardo para obtener clones 406, 407 del

elemento original 405 correspondiente al elemento j dentro de la misma cadena. Por tanto, es más fácil garantizar el equilibrio que en una PUF árbitro ya que los diferentes caminos de un elemento de retardo no se cruzan.

[0048] Los elementos de retardo no poseen las mismas características físicas de una cadena a otra, introduciendo así retardos diferentes que la LPUF puede explotar.

[0049] La figura 5 presenta una LPUF que comprende N = 2 cadenas de retardo. Las dos cadenas de retardo 500, 501 comprenden cada una de ellas M elementos de retardo. Estas cadenas de retardo son idénticas topológicamente, esto es, funcionalmente, y poseen la misma estructura física. Los elementos de retardo 506, 507, así como su interconexión 508, se encuentran nuevamente de idéntica forma en la segunda cadena de retardo 501. Las cadenas están unidas en serie entre ellas y la salida de la segunda está cerrada en la entrada de la primera con ayuda de una línea de bucle 502. Una puerta lógica 503 que realiza una función de inversión se sitúa en dicho bucle 502. Este conjunto cerrado constituye un oscilador configurable.

[0050] Los dos elementos de retardo 500, 501 son controlados respectivamente por dos palabras binarias C_1 y C_2.

[0051] C_1 y C_2 están compuestos cada uno de ellos por M bits respectivamente con las referencias $C_{1,1}$, $C_{1,2}$, …, $C_{1,M}$, y $C_{2,1}$, $C_{2,2}$, …, $C_{2,M}$. Estas dos palabras son generadas por un módulo de control 505.

[0052] La frecuencia de la señal de salida de la última cadena de retardo es analizada por un módulo de medición 504. El valor de frecuencia medida depende de los retardos introducidos por las diferentes cadenas de retardo aplicándoles, por consiguiente, palabras de control. El módulo de control 505 aplica, por ejemplo, sucesivamente un primer valor del par $(C_1, C_2) = (0, 2^j)$, esto es, que $C_{2,j} = 1$ ($j\varepsilon[1;M]$) y los otros bits de C_1 y C_2 son iguales a cero, y a continuación un segundo valor del par $(C_1, C_2) = (2^j, 0)$.

[0053] El módulo de medición 504 mide sucesivamente las frecuencias de las señales que corresponden a la aplicación de los dos valores del par (C_1, C_2), estando indicadas dichas medidas respectivamente con las referencias $freq(0, 2^j)$ y $freq(2^j, 0)$. De estas medidas se deducen cantidades representativas de los bits de la firma. Por ejemplo, una diferencia de frecuencia δ_j es estimada seguidamente por el módulo de control 505 utilizando la siguiente expresión:

$$\delta_j = freq(0,2^j) - freq(2^j,0) \qquad (1)$$

[0054] La diferencia de retardo de propagación en las cadenas de retardo, consecuencia de la aplicación de los dos valores del par (C_1, C_2) que modifican el camino tomado por la señal, no es nula y puede ser explotada. En efecto, esta diferencia de retardo supone la diferencia en frecuencia medida δ_j, pudiendo ser, por tanto, utilizada esta última especialmente para la generación de los bits de la firma propia al circuito.

[0055] De este modo, se puede elegir un convenio para generar los bits de la firma a partir de las cantidades representativas δ_j de los bits de la firma. Por ejemplo, si N = 2, el bit i es igual a 0 si δ_j es positivo e igual a 1 si δ_j es negativo.

[0056] Con el fin de generar los diferentes bits de la firma, se presentan palabras binarias denominadas más adelante en la descripción “palabras de desafío” a la entrada de la LPUF que son tratadas por el módulo de control 505. El módulo de control 505 genera sobre esta base combinaciones de palabras de control utilizadas para configurar las cadenas de retardo y para que las diferencias de frecuencia puedan ser medidas. En efecto, una palabra de desafío está compuesta por N palabras de control. Estas palabras de control pueden ir combinadas de diferentes formas según N! combinaciones de control posibles de las N palabras C_i, representando el punto de exclamación la operación factorial, con el fin de obtener tantas configuraciones de las cadenas de retardo como sean posibles. Una respuesta es entonces determinada, por ejemplo, por el módulo de control. Para N=2, un ejemplo de respuesta que corresponde a la firma del circuito puede ser expresada en función de la diferencia de frecuencia mencionada anteriormente. Si N>2, una respuesta puede estar determinada, por ejemplo, en función del orden de las frecuencias para las N ! combinaciones de control posibles.

[0057] Con el fin de comparar y seleccionar las frecuencias obtenidas para diferentes combinaciones de control y, por lo tanto, de retardo, debe haber al menos dos combinaciones de palabras C_i diferentes. Si se considera la distancia de Hamming total HD de la combinación de palabras C_i, HD se expresa utilizando la expresión:

$$HD = \sum_{i=1,i'>i}^{i=N} HW(C_i \oplus C_{i'}) \quad i,i' \in [1,N] \qquad (2)$$

en la que:

HW() es una función que determina el peso de Hamming;

$\oplus$ representa la operación lógica OU exclusivo.

[0058] Si (C_1, $C_{i'}$) son dos palabras de control establecidas a partir de una combinación de palabras que actúa sobre N cadenas, la condición expresada por la siguiente expresión debe ser preferentemente comprobada para tener la certeza de disponer al menos de dos combinaciones posibles:

$$\forall i,i' \in [1,N] \quad HD \geq 1 \qquad (3)$$

[0059] Además, el bit j de las N cadenas de retardo no debe permanecer en el valor "1"; de lo contrario ninguna diferencia de bits podrá ser detectada por el controlador. El bit j puede seguir siendo igual a "0" por convenio. Por ejemplo, si N=2 y M=3, la diferencia δ_j obtenida por el valor del par (C_1, $C_{2,}$) = (0, 1) es el mismo que para los valores del par (C_1, $C_{2,}$) = (2, 3), (C_1, $C_{2,}$) = (4, 5) y (C_1, $C_{2,}$) = (6, 7). En otros términos, la siguiente expresión debe ser verificada:

$$\forall j \in [1,M] \qquad \prod_{i=1}^{N} (C_{i,j}) = 0 \qquad (4)$$

[0060] Una LPUF puede igualmente incluir un mecanismo de protección contra los ataques por observación o por inyección de fallos. Para ello, se puede integrar un generador de números aleatorios en el circuito. Este puede ser utilizado para seleccionar el orden en el que son medidas las frecuencias. De este modo, el atacante no puede ni forzar un valor de bit ni conocer el valor de un bit ya que la medición de las frecuencias se realiza en una secuencia aleatoria de palabras de control.

[0061] Ventajosamente, una LPUF es resistente a los ruidos e interferencias relacionados con el entorno. En efecto, el ruido de perturbación afecta de manera idéntica a las cadenas de retardo que componen la LPUF. Por tanto, el resultado de las medidas de frecuencia se ve escasamente afectado por este ruido si es de duración superior a la medición y, por consiguiente, se mantiene fiable la generación de la firma, lo que puede no ser el caso para las PUF de pares de osciladores en anillo.

[0062] Para una aplicación destinada a la autentificación de un circuito, una LPUF puede ser utilizada con un mecanismo CRP, acrónimo procedente de la expresión anglosajona "Challenge-Response Pair".

[0063] Este mecanismo puede ser aplicado integrando una LPUF a dicho circuito. Se presenta un mensaje o palabra de desafío ("challenge" en inglés) en dicha LPUF, y esta determina a continuación un mensaje de respuesta que permite autentificar el circuito. Efectivamente, este mensaje de respuesta corresponde a una firma generada por la PUF y es propia a dicho circuito.

[0064] Una LPUF puede ser igualmente utilizada para la generación de una clave de cifrado. Para ello, la LPUF utiliza ella misma un subconjunto de mensajes de desafío, y la firma de este modo generada puede ser utilizada como clave de cifrado.

[0065] Una palabra de desafío corresponde a la concatenación de N palabras de control C_i ($i\varepsilon[1, ..., N]$), estando utilizada una palabra de control para cada una de las N cadenas de retardo. La palabra de respuesta es el resultado de las mediciones y comparaciones de frecuencia resultantes de las N! combinaciones posibles de las N palabras Ci, representando el punto de exclamación la operación factorial. Para obtener N! combinaciones diferentes cabe la posibilidad de añadir a las condiciones (3) y (4) el hecho de que todas las palabras de control Ci son diferentes. Esto se puede expresar mediante la fórmula:

$$i,i' \in [1,N] \quad \prod_{i \neq i} (C_i \oplus C_{i'}) \geq 1 \qquad (5)$$

[0066] Las frecuencias medidas son comparadas entre ellas de manera que se configura una respuesta conforme a un protocolo dado. Por ejemplo, las N! combinaciones pueden ser seleccionadas de modo diferente para obtener (N!)! configuraciones.

[0067] La figura 6 muestra un ejemplo de método de combinación de las palabras de control utilizadas en una LPUF. En este ejemplo, N=3 y las palabras de control C_i pueden adoptar tres valores A, B y C 600 respetando las condiciones (3), (4) y (5). De este modo, pueden generarse 6 combinaciones posibles 603 para las palabras de control (C1, C2, C3), pudiendo obtenerse 720 configuraciones de frecuencia.

[0068] Ventajosamente, el número de palabras de desafío posibles es significativamente más importante que para una PUF árbitro. En efecto, para una PUF árbitro éste tiene un valor de 2^M. Para una LPUF, y considerando las expresiones (3), (4) y (5), el número de palabras de desafío posibles es dado por la siguiente tabla (1) para ciertos valores de N y M:

Tabla (1): Número de palabras de desafío posibles

	M									
	2	3	4	5	6	7	8	10	12	16
Árbitro	4	8	16	32	64	128	256	1K	4K	64K
LPUF N=2	4	13	40	121	364	1093	3280	29524	~250K	~21M
LPUF N=3	4	44	360	2680	19244	~130K	~1M	~45M	~2G	~5000G

[0069] Ventajosamente, el número de firmas diferentes que pueden ser generadas es, por tanto, muy elevada para una LPUF en comparación con una PUF árbitro.

[0070] Para una aplicación destinada a generar una clave de cifrado intrínseca al componente en el que está implementada la LPUF, un método consiste en utilizar palabras de control predefinidas, esto es, palabras de control memorizadas por el circuito. El principio es el mismo que la autentificación con la diferencia de que no se produce el envío de palabras de desafío, sino que le corresponde a la LPUF considerar un subconjunto de palabras de desafío sobre las que se miden y comparan las frecuencias de las combinaciones.

[0071] Con el fin de ilustrar el principio de este método, consideramos un módulo de control de la LPUF utilizando palabras de control Ci idénticas cuyos bits son forzados a cero, salvo para una palabra de control en la que uno de los bits adquiere el valor 1. E valor asociado a esta palabra de control es 2^j, designando j al elemento j de retardo utilizado para generar un bit de la clave. El módulo de control de la LPUF genera a continuación N! combinaciones aplicando una permutación sobre las N palabras de control Ci. Como en este ejemplo todas las palabras de control son idénticas (cero) salvo una, el número de combinaciones es igual a N y no a N!. Las N frecuencias que corresponden a estas N combinaciones son obtenidas mediante mediciones.

[0072] Un valor de frecuencia medido corresponde a una combinación de palabras de control (C_1 …, C_N), el cual aparece como freq(C_1 …, C_N). De este modo, las N frecuencias f_1, f_2, …, f_N corresponden a las N combinaciones mencionadas anteriormente y pueden expresarse de la siguiente forma:

$$f_1 = \text{freq}(0,0,...,2^j)$$

...

$$f_{N-1} = \text{freq}(0,2^j,...,0)$$

$$f_N = \text{freq}(2^j,0,...,0)$$

[0073] Estas frecuencias medidas son seleccionadas, por ejemplo, de forma que a una diferencia o una combinación de frecuencias medidas corresponda un bit de la firma que se va a generar.

[0074] A título de ejemplo, si N=2, una diferencia de frecuencias δ_i permite obtener el bit j de la clave de cifrado, pudiendo ser determinada esta diferencia utilizando la expresión (1).

[0075] En el caso en el que N=3, hay 3 valores de frecuencias posibles y, por consiguiente, seis combinaciones posibles. Los tres valores son:

$$f_1 = \text{freq}(0,0,2^j)$$

$$f_2 = \text{freq}(0,2^j,0)$$

$$f_3 = \text{freq}(2^j,0,0)$$

[0076] Los bits de la clave de cifrado pueden ser seguidamente deducidos con la ayuda de una tabla que facilitamos a continuación a modo de ejemplo:

Tabla(2) : ejemplo de correspondencia entre frecuencias medidas y bits de la firma

Combinación de frecuencias medidas			Bit de la clave
f_1	f_2	f_3	1
f_1	f_3	f_2	1
f_2	f_3	f_1	0
f_3	f_2	f_1	0
f_3	f_1	f_2	0
f_2	f_1	f_3	1

[0077] Este mismo método puede aplicarse utilizando palabras de desafío predefinidas para obtener la firma. El numero de palabras de desafío está relacionado con el número de bits que pueden ser extraídos para constituir una clave de cifrado o una palabra de respuesta utilizada para autentificar el circuito que incluye la LPUF.

[0078] Por ejemplo, si N=2 y M=5, considerando la tabla (1), es posible obtener 121 bits diferentes.

[0079] Si N es superior a 2, el número de bits que pueden obtenerse aumenta rápidamente ya que existe (N!)! configuraciones posibles, tal como se ha explicado previamente en la descripción.

[0080] El número máximo de bits que componen la firma es igual al número de palabras de desafío posibles multiplicado por el logaritmo en base 2 de (N !) !. La tabla (1) muestra que existe un número muy importante de palabras de desafío y, por tanto, de bits de firma. No obstante, estos pueden resultar redundantes ya que las palabras de desafío pueden compartir las mismas combinaciones de bits, por ejemplo si N=3, la palabra de desafío M1=(0, 1, 2) es próxima a la palabra de desafío M2= (0, 1, 3). Esta redundancia se mantiene débil eligiendo combinaciones de palabras de control con distancias muy grandes entre ellas. De este modo, esta elección puede ser realizada, por ejemplo, respetando un requisito de distancia de tal forma que la distancia de Hamming entre una palabra de desafío y las N! combinaciones de las otras palabras no sea inferior a un valor mínimo. En el ejemplo anterior, la distancia entre M1 y M2 es de HW[(0,1,2) $\oplus$ (0,1,3)] = 1. Si el valor mínimo elegido es de 2, una de estas palabras de desafío será rechazada.

[0081] El circuito LPUF puede incluir un bit de paridad. En efecto, especialmente a causa de las características físicas del circuito tras su fabricación, uno de los bits de la firma puede ser generado de manera errónea.

[0082] El bit de paridad es calculado por el circuito sobre el conjunto de los bits de la firma. Un convenio que puede ser utilizado es el de posicionar el bit de paridad a “0” si el número de bits de la firma a “1” es par.

[0083] Puede utilizarse una memoria no volátil con el fin de proteger este bit. Si se utiliza un circuito FPGA, basta con disponer de 2 ficheros de configuración propios a cada valor del bit de paridad.

[0084] Con el fin de reducir la probabilidad de generar un bit de firma erróneo, el módulo de medición de la LPUF puede efectuar de manera sucesiva diversas mediciones de las cantidades representativas de los bits de firma, denominadas igualmente ensayos, para una combinación de control dada. Los valores obtenidos gracias a estos ensayos son a continuación acumulados y el signo del resultado acumulado da el bit de firma.

[0085] Cuando un bit de paridad está asociado al funcionamiento de la LPUF, el bit menos fiable puede ser detectado fácilmente durante el tratamiento correspondiente a los ensayos.

[0086] Este bit puede entonces ser corregido fácilmente invirtiéndolo si resulta que no se ha respetado la paridad.

[0087] Este principio queda ilustrado con ayuda de la figura 8, en el que una de las curvas 800 corresponde al bit menos fiable y las otras curvas corresponden a bits más fiables de la firma. Tal y como se ha explicado anteriormente, en el momento en que la medición ha finalizado, el bit no fiable puede ser corregido si la paridad no se ha respetado.

[0088] Las características de las LPUF pueden ser utilizadas con el fin de aplicar un procedimiento que permita realizar un test y/o seleccionar los circuitos integrados con una probabilidad despreciable de generar una firma errónea. De este modo, este procedimiento permite aumentar la fiabilidad de utilización de las LPUF ya que permite especialmente excluir los circuitos no fiables así como seleccionarlos por nivel de fiabilidad, pudiendo utilizarse un circuito con un nivel de fiabilidad dado para una familia de aplicaciones dada. Este procedimiento puede ser aplicado, por ejemplo, al final del proceso de fabricación de los circuitos con el fin de conservar únicamente aquellos circuitos que resulten más fiables.

[0089] Ventajosamente, esta posibilidad de seleccionar los circuitos permite evitar la implementación de un código corrector de error.

[0090] El procedimiento tiene especialmente como objeto excluir los circuitos que tengan una probabilidad de generar una firma errónea superior a un valor dado de probabilidad.

[0091] Más adelante en la descripción se describe un ejemplo de aplicación del procedimiento. En este ejemplo, se considera un circuito que incluye una LPUF. La LPUF contiene N=2 cadenas de retardo, estando deducido cada bit de firma de la medición de diferencia de frecuencia δ_j tal como se ha definido previamente.

[0092] Considerando una población de circuitos que hayan sido fabricados de forma idéntica, la variable δ_j sigue una distribución gaussiana de media nula y de varianza σ^2, esto es:

$$\delta_j \in N(0, \sigma^2) \qquad (6)$$

N(a, b) representa una ley gaussiana de media a y de varianza b.

[0093] A nivel del circuito, cada medida δ_j es sensible al entorno. Un valor medido de δ_j correspondiente al bit j de la firma del circuito aparece con la referencia $\hat{\delta}_j$ y sigue una distribución gaussiana centrada en δ_j y de varianza s^2 que corresponde al ruido de medición, esto es:

$$\hat{\delta}_j \in N(\delta_j, s^2) \qquad (7)$$

[0094] El valor de δ_j debe estar lo más alejado posible de 0 con el fin de obtener un valor fiable de la medición $\hat{\delta}_j$ La probabilidad de error en el bit j indicado como $P_{e,j}$ corresponde, por ejemplo, a la probabilidad de que el signo del valor medido $\hat{\delta}_j$ sea diferente del signo del valor esperado δ_j. Esta probabilidad puede expresarse utilizando la siguiente expresion:

$$P_{e,j} = \frac{1}{2}\left(1 - \mathrm{erf}\left(\frac{\delta_j}{s\sqrt{2}}\right)\right) \qquad (8)$$

En la que la función erf() es la función de error de Gauss.

[0095] Un ejemplo gráfico que representa este error queda ilustrado en la figura 7. $P_{e,j}$ corresponde a una superficie 701 correspondiente a la integración entre -∝ y 0 de la densidad de probabilidad de $\hat{\delta}_j$ 700.

[0096] Esta probabilidad de error $P_{e,j}$ es significativa si δ_j es próximo a 0. Puede ser reducida en la práctica efectuando un número T de ensayos durante los cuales los resultados de las mediciones son acumulados. De este modo, se realizan T mediciones $\hat{\delta}_i$. $P_{e,j}$ puede expresarse utilizando la siguiente expresión:

$$P_{e,j} = \frac{1}{2}\left(1 - erf\left(\frac{\sqrt{T} \times \delta_j}{s\sqrt{2}}\right)\right) \qquad (9)$$

[0097] De este modo, si δ_j es débil y superior a un valor umbral Th, deberá aplicarse un número significativo T de ensayos si la probabilidad de error deseada es débil. Fijándose un umbral de Th, resulta así posible eliminar los circuitos con δ_j inferiores a Th, poseyendo una cierta probabilidad de error y respetando el número de ensayos que se van a realizar. Th puede ser ventajosamente elegido teniendo en cuenta las condiciones desfavorables en términos de temperatura y de tensión de alimentación del circuito.

[0098] Si se considera un circuito con un número M de elementos de retardo asociados cada uno a un bit de firma, basta con que haya al menos un bit j como $\delta_j < Th$ para que el circuito sea rechazado. La probabilidad de que un circuito testado sea rechazado en este ejemplo puede, por tanto, predecirse utilizando la siguiente expresión:

$$P_{rej} = 1 - \left[1 - P(|\delta_i| < Th)\right]^M \qquad (10)$$

en la que:

$$P(|\delta_i| < Th) = erf\left(\frac{Th}{\sqrt{2} \times \sigma}\right). \qquad (11)$$

El ejemplo arriba expuesto corresponde a N=2 y las palabras de control con un solo bit j al valor 1. La probabilidad de error disminuye si N>2 o si las palabras de control contienen diversos bits no nulos con una cierta distancia de Hamming HD entre ellas, tal y como se expresa en la ecuación (12).

[0099] De este modo, un bit de firma está correlacionado con HD elementos de retardo que sirven para generar la diferencia entre dos mediciones de frecuencias. Es equivalente a considerar que la medición consiste en la suma de HD valores de δ_j. De ello se desprende que:

$$P(|\delta_i| < Th) = erf\left(\frac{Th}{\sqrt{2.HD} \times \sigma}\right) \qquad (12)$$

Aumentar la distancia de Hamming HD entre las palabras de control utilizadas permite, por tanto, disminuir la probabilidad de rechazo de los circuitos P_{rej}.

El número B de bis de firma puede entonces ser bastante superior a M. El índice de rechazo en este caso es idéntico a la expresión aunque reemplazando M por el número efectivo de bits B de la firma:

$$P_{rej} = 1 - \left[1 - \mathrm{erf}\left(\frac{Th}{\sigma \times \sqrt{2 \times HD}} \right) \right]^{B} \qquad (13)$$

[0100] El procedimiento según la invención efectúa una serie de mediciones que pueden ir hasta T ensayos, y acumular a continuación los resultados $\hat{\delta}_j$ de dichas mediciones para cada bit. Los valores obtenidos gracias a estos ensayos son comparados con uno o varios valores umbral predefinidos. El resultado de esta comparación permite decidir si el bit de la firma para el que se han realizado los ensayos corresponde a 0, a 1, o a un valor indeterminado cuando no se ha alcanzado el umbral, en cuyo caso el bit es considerado indeterminado o no fiable. Un valor indeterminado es un valor que no permite decidir si el bit está a "0" o a "1". Esta técnica permite dar fiabilidad a los resultados de las mediciones utilizadas para la generación de los bits de la firma y, por consiguiente, reducir la probabilidad de que un bit de dicha firma sea generado con un error.

[0101] Ventajosamente, el tiempo de medición puede ser optimizado si el módulo de control de la LPUF detiene el cálculo para un bit de firma dado cuando se alcanza un cierto valor umbral.

[0102] Para N=2 las mediciones corresponden, por ejemplo, a las diferencias δ_j que se han definido anteriormente. De este modo, dos valores umbral pueden ser elegidos y comparados con los resultados de las mediciones acumuladas para cada bit de la firma, correspondiendo estos dos umbrales, por ejemplo, a los valores:

- ThxT, para el cual se elige un 1 si una medición acumulada es superior a este valor;
- -ThxT, para el cual se elige un 0 si una medición acumulada es inferior a este valor.

[0103] Cuando la acumulación de los resultados de medición que corresponden a un bit dado de la firma del circuito alcanza uno de estos valores umbral, las mediciones se detienen y se toma una decisión en cuanto al valor del bit.

[0104] El principio de mediciones sucesivas y de comparación con un umbral puede ser aplicado en el marco del procedimiento de test de circuitos, aunque también por los propios circuitos, tal y como se explicado previamente.

[0105] Para un circuito considerado como fiable una vez aplicado el procedimiento de test según la invención, habrá sistemáticamente convergencia. Los bits más fiables convergerán rápidamente y los menos fiables requerirán más ensayos de mediciones.

[0106] Cuando se aplica el procedimiento de test a circuitos que contienen una LPUF que incluye un bit de paridad asociado a la firma, el índice de rechazo puede verse significativamente reducido. En efecto, el método de test no rechazará los circuitos que posean un bit de firma no fiable, esto es, para el que $\delta_j < Th$.

[0107] La figura 9 muestra un ejemplo de combinaciones de palabras de control y de comparación de las medidas de frecuencia asociadas que permiten reducir el índice de rechazo de un circuito que contiene una LPUF. Cuando N > 2, existe la posibilidad de utilizar una medición independiente de la temperatura empleando las relaciones entre diferencias de frecuencias antes que diferencias entre mediciones. Los bits de la firma del circuito son entonces deducidos del valor de esas relaciones. La figura 9 muestra las 6 combinaciones posibles de tres palabras de control (A, B, C) para N=3.

[0108] En este caso, los bits de firma son deducidos de una métrica $\Delta_{i,j}$ que corresponde, por ejemplo, a:

$$\Delta_{i,j} = \frac{\delta_i}{\delta_j} \qquad (14)$$

[0109] En esta ecuación, los valores δ_i y δ_j corresponden a las diferencias de las frecuencias medidas, estando medida una diferencia entre dos combinaciones distintas de palabras de control.

[0110] El módulo de control de la LPUF determina entonces la métrica $\Delta_{i,j}$ de la que deduce un bit de la firma del circuito. El ejemplo de la figura 9 muestra un ejemplo en el que el primer bit b_0 de la firma está posicionado en 1 si $\Delta_{1,2} > 0$, valiendo 0 en el caso contrario. Del mismo modo, el segundo bit b_1 de la firma está posicionado en 1 si $\Delta_{3,4} > 0$, valiendo 0 en el caso contrario.

[0111] La figura 10 muestra un ejemplo del procedimiento de test de circuitos según la invención.

[0112] Una primera etapa del procedimiento 1000 tiene como objeto seleccionar los parámetros de configuración del test. De este modo, los valores de los parámetros T y Th definidos previamente pueden ser seleccionados, influyendo dichos valores en la probabilidad de seleccionar o rechazar un circuito así como en la duración del test. Esta etapa de configuración permite igualmente seleccionar B combinaciones de palabras de control de modo que se garantice una distancia Hamming HD entre dos combinaciones de este conjunto de B combinaciones.

[0113] Una segunda etapa 1001 del procedimiento tiene como objeto determinar la probabilidad de error por bit, así como la probabilidad de rechazo de los circuitos testados. Estas dos probabilidades son determinadas utilizando, por ejemplo, las expresiones (9) y (13) considerando, por una parte, los parámetros T y Th elegidos en la etapa de configuración y, por otra, los valores medidos 1002 de la varianza del ruido de medición s^2 y de la varianza σ^2 de las mediciones debida a la dispersión de tratamiento. La medición de estas varianzas puede ser efectuada por cualquier medio de medición conocido por el experto en la materia.

[0114] La determinación de estas probabilidades permite ventajosamente adaptar el valor de los parámetros de configuración en función de las necesidades del usuario.

[0115] Una tercera etapa 1003, denominada la etapa de medición, tiene como objeto determinar si el circuito testado es considerado fiable. Si no es el caso, dicho circuito es rechazado. Esta fase de medición es aplicada a todos los circuitos a los que el usuario ha decidido realizar el test. Para ello, el módulo de control de la LPUF contenida en el circuito que se pretende verificar es configurado de modo que se apliquen las B combinaciones de palabras de control seleccionadas en la primera fase con el fin de permitir las mediciones de las diferencias de frecuencias δ_j. Se efectúan numerosos ensayos para cada bit de la firma para ser acumulados y comparados con uno o varios valores umbral, tal y como se ha descrito previamente.

[0116] Si la LPUF no tiene a su disposición ningún bit de paridad, el circuito es rechazado si al menos uno de los bits no se considera fiable.

[0117] En el caso de que la LPUF tenga a su disposición un bit de paridad, el circuito testado para el que un único bit de la firma no se ha considerado fiable, no será rechazado, y se calculará un valor del bit de paridad sobre la firma así generada. Ello permitirá posteriormente al circuito detectar un error en un bit no fiable y corregirlo.

[0118] Cabe mencionar que para optimizar la fiabilidad de este método de test, las mediciones de las varianzas s_2 y σ^2, así como la fase de medición pueden ser ventajosamente efectuadas en las condiciones que corresponda a las condiciones extremas de funcionamiento de los circuitos testados. Estas condiciones corresponden, por ejemplo, a una temperatura sensiblemente igual a +70ºC y una tensión de alimentación sensiblemente inferior al 5% con respecto a la tensión de alimentación nominal del circuito testado.

[0119] La figura 11 muestra un ejemplo de sistema de test que aplica el procedimiento de test según la invención. El sistema de test 1100 está compuesto, por ejemplo, por un ordenador 1105 provisto de una interfaz de usuario 1104. El sistema incluye igualmente un equipo 1101 que permite controlar las sondas de medición 1106, 1107. Estas sondas de medición están conectadas a una tarjeta electrónica 1102 que contiene el circuito electrónico al que pretende realizarse el test 1103, incluyendo dicho circuito una LPUF. El sistema aplica el procedimiento de test descrito anteriormente. La interfaz de usuario 1104 permite configurar el test así como mostrar los resultados.

Reivindicaciones

1. Circuito integrado de silicio que incluye una función físicamente no reproducible LPUF que permite la generación de una firma propia a dicho circuito, estando dicha función **caracterizada porque** incluye:

- un oscilador en anillo compuesto por un bucle (502) recorrido por una señal e, estando formado dicho bucle por N cadenas de retardo (500, 501) topológicamente idénticas, conectadas en serie entre ellas, y una compuerta de inversión (503), estando compuesta una cadena de retardo (500, 501) por M elementos de retardo (506, 507) conectados en serie entre ellos;
- un módulo de control (505) que genera N palabras de control (C_1, C_2), estando utilizadas dichas palabras para configurar el valor del los retardos introducidos por las cadenas de retardo en la señal e que les recorre;
- un módulo de medición (504) que mide la frecuencia de la señal a la salida de la última cadena de retardo (501) tras la actualización de las palabras de control;
- medios para deducir de las medidas de frecuencia los bits que componen la firma del circuito.

2. Circuito según la reivindicación 1, **caracterizado porque** el circuito es un ASIC o un FPGA.

3. Circuito según una de las reivindicaciones 1 o 2, **caracterizado porque** la firma es utilizada como clave de cifrado.

4. Circuito según una de las reivindicaciones 1 o 2, **caracterizado porque** la firma es utilizada para su autentificación.

5. Circuito según una de las reivindicaciones precedentes, **caracterizado porque** los elementos de retardo incluyen medios para bifurcar (400) la señal que les recorre ($e_{i,j}$) según al menos dos caminos distintos (403, 404), introduciendo un camino un valor de retardo ($d_{i,j}^0$, $d_{i,j}^1$) que le es propio, estando controlada esta separación por al menos un bit ($C_{i,j}$) que pertenece a una palabra de control.

6. Circuito según una de las reivindicaciones precedentes, **caracterizado porque** las palabras de desafío compuestas por una concatenación de palabras de control son presentadas a la entrada del módulo de control (505), generando dicho módulo combinaciones a partir de dichas palabras con el fin de configurar las cadenas de retardo (500, 501).

7. Circuito según una de las reivindicaciones precedentes, **caracterizado porque** los bits de la firma se determinan en función de la clase de las frecuencias medidas por las diferentes combinaciones de palabras de control.

8. Circuito según una de las reivindicaciones 1 a 6, **caracterizado porque** los bits de la firma se determinan en función de las diferencias estimadas (δ_j) entre dos valores de frecuencia medidos, correspondiendo un valor de frecuencia medido a una combinación de palabras de control.

9. Circuito según una de las reivindicaciones 1 a 6, **caracterizado porque** los bits de la firma se determinan en función del valor de la relación entre dos diferencias de frecuencia estimadas (δ_j).

10. Circuito según una de las reivindicaciones precedentes, **caracterizado porque** incluye un generador de números aleatorios, siendo utilizados los números aleatorios con el fin de seleccionar el orden en el que son medidas las frecuencias correspondientes a las combinaciones de palabras de control.

11. Circuito según una de las reivindicaciones precedentes, **caracterizado porque** contiene al menos un bit de paridad, siendo utilizado dicho bit para corregir un bit de la firma generado con un error.

12. Procedimiento de test de circuitos integrados que incluye una función físicamente no reproducible LPUF según una de las reivindicaciones 1 a 11, **caracterizado porque** se aplica una sucesión de etapas a los circuitos testados de modo que se seleccionen los circuitos permitiendo generar una firma propia a dicho circuito con un nivel de fiabilidad elegido, correspondiendo dichas etapas a:

- una selección de los parámetros T y Th (1000) de configuración del test, así como de B combinaciones de palabras de control con una distancia de Hamming al menos igual a un valor predefinido HD;
- una fase de mediciones (1003) durante la cual se miden cantidades representativas (δ_j) de los bit de firma del circuito, realizándose hasta T mediciones por bit de firma, estando acumuladas esas T mediciones de modo que se decida si el bit correspondiente es indeterminado, habiendo tomado la decisión tras la comparación con al menos un valor deducido del valor del parámetro Th, estando seleccionados los circuitos testados en función del número de bits indeterminados detectados.

13. Procedimiento según la reivindicación 12, **caracterizado porque** incluye una etapa de determinación de la probabilidad para que un circuito no sea seleccionado, estando determinada dicha probabilidad utilizando la expresión:

$$P_{rej} = 1 - \left[1 - \mathrm{erf}\left(\frac{Th}{\sigma \times \sqrt{2 \times HD}} \right) \right]^{B}$$

en la que:

erf() es la función de error de Gauss;
σ es la varianza de las mediciones de las cantidades representativas de los bits de firma del circuito.

14. Procedimiento según una de las reivindicaciones 12 o 13, **caracterizado porque** incluye una etapa de determinación de la probabilidad de error por bit de firma, estando determinada dicha probabilidad utilizando la expresión:

$$P_{e,j} = \frac{1}{2}\left(1 - erf\left(\frac{\sqrt{T} \times \delta_j}{s\sqrt{2}} \right) \right)$$

en la que:

δ_j es una diferencia de frecuencia medida entre dos frecuencias que corresponden a la aplicación de dos combinaciones de palabras de control distintas;
s, definida como s^2, es la varianza del ruido de medición.

15. Procedimiento según una de las reivindicaciones 12 a 14, **caracterizado porque** un circuito es seleccionado si ningún bit de la firma es indeterminado.

16. Procedimiento según una de las reivindicaciones 12 a 14, **caracterizado porque** cuando la función LPUF de un circuito testado está asociada a un bit de paridad cuyo valor está determinado a partir de la firma de dicho circuito, dicho circuito es seleccionado si el número de bit indeterminado es estrictamente inferior a 2.

17. Procedimiento según una de las reivindicaciones 12 a 16, **caracterizado porque** los valores de s^2 y σ^2 son medidos (1002) para una temperatura sensiblemente igual a +70Cº y una tensión de alimentación de los circuitos sensiblemente inferior al 5% con respecto a la tensión de alimentación nominal, estando efectuada la fase de mediciones (1003) en las mismas condiciones.

18. Sistema de test que aplica el procedimiento según una de las reivindicaciones 13 a 17, **caracterizado porque** está compuesto por un ordenador (1105) provisto de una interfaz de usuario (1104), un equipo (1101) que permite controlar las sondas de medición (1106, 1107), teniendo dichas sondas la función de recopilar las mediciones de las cantidades representativas (δ_j) de los bits de firma producidas por los circuitos testados (1103), estando a continuación efectuados los tratamientos asociados a esta fase por el ordenador (1105) y mostrados en su interfaz (1104).

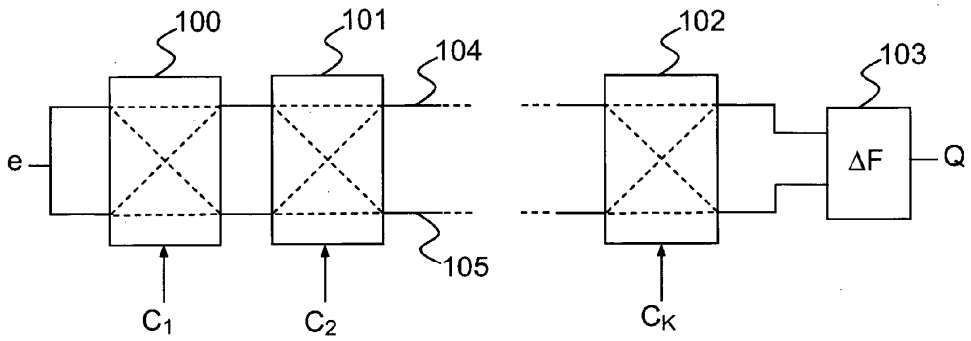

FIG.1

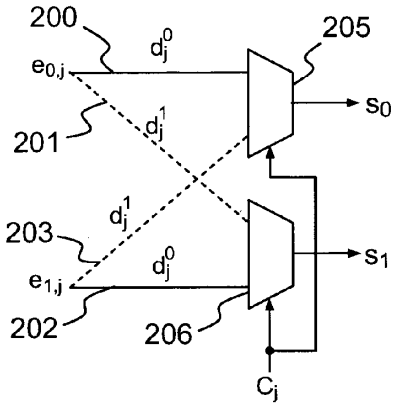

FIG.2

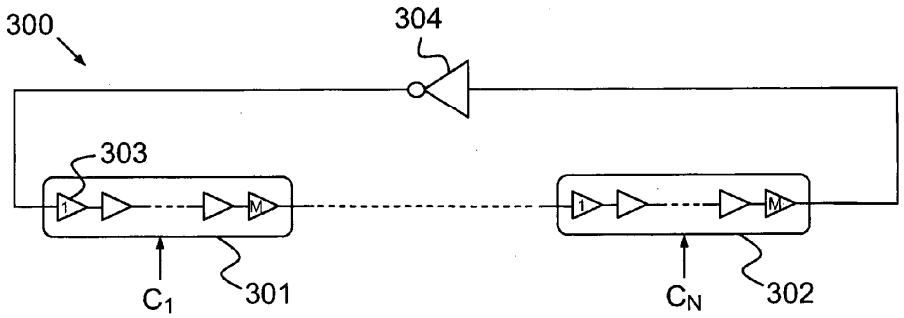

FIG.3

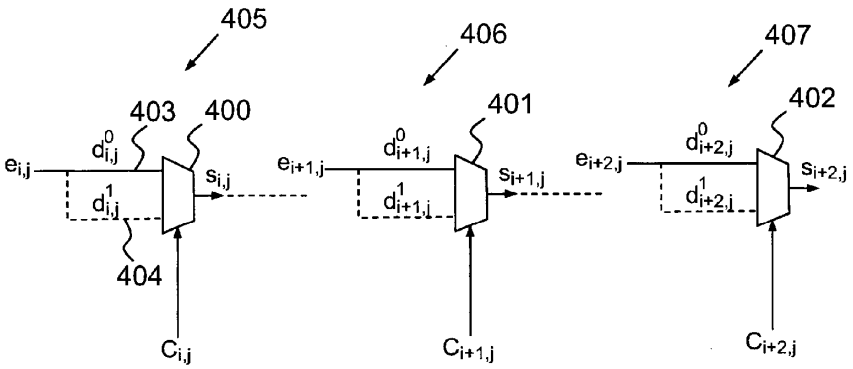
405
406
407
403
400
401
402
$e_{i,j}$
$d^0_{i,j}$
$d^1_{i,j}$
$s_{i,j}$
$e_{i+1,j}$
$d^0_{i+1,j}$
$d^1_{i+1,j}$
$s_{i+1,j}$
$e_{i+2,j}$
$d^0_{i+2,j}$
$d^1_{i+2,j}$
$s_{i+2,j}$
404
$C_{i,j}$
$C_{i+1,j}$
$C_{i+2,j}$

FIG.4

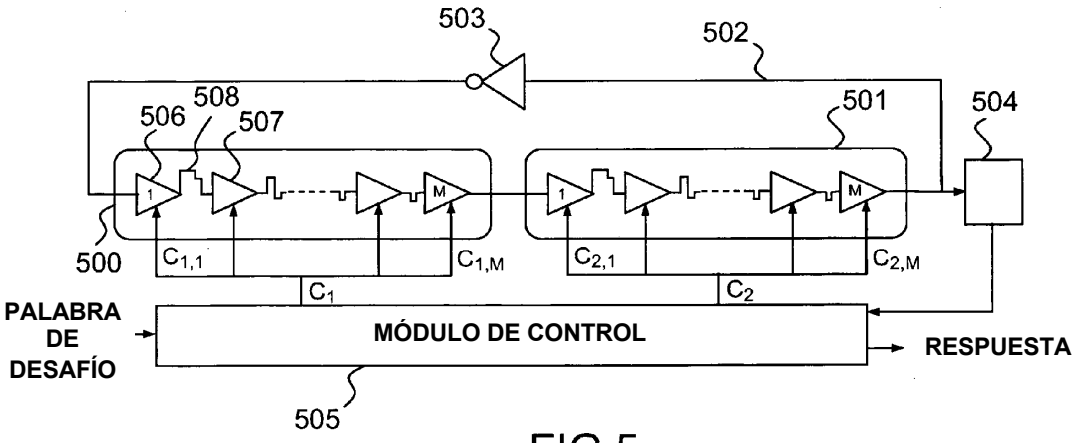
503
502
508
506
507
501
504
1
M
500
$C_{1,1}$
$C_{1,M}$
$C_{2,1}$
$C_{2,M}$
C_1
C_2
PALABRA DE DESAFÍO
MÓDULO DE CONTROL
RESPUESTA
505

FIG.5

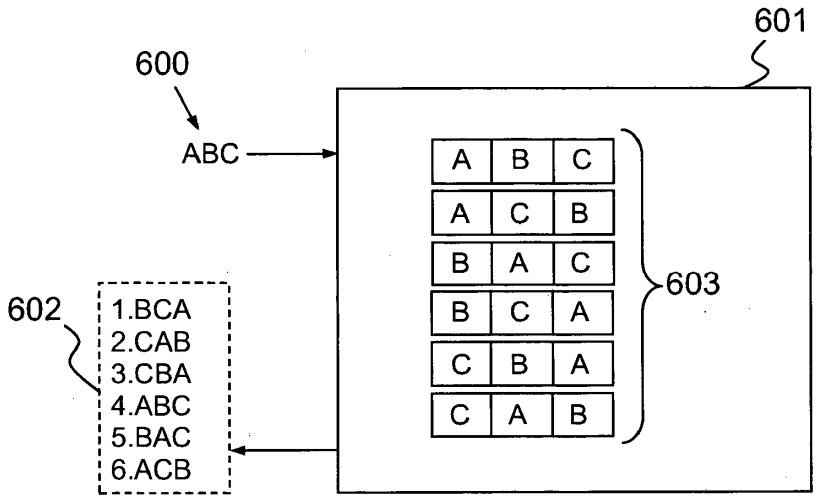
601
600
ABC
A B C
A C B
B A C
B C A
C B A
C A B
603
602
1.BCA
2.CAB
3.CBA
4.ABC
5.BAC
6.ACB

FIG.6

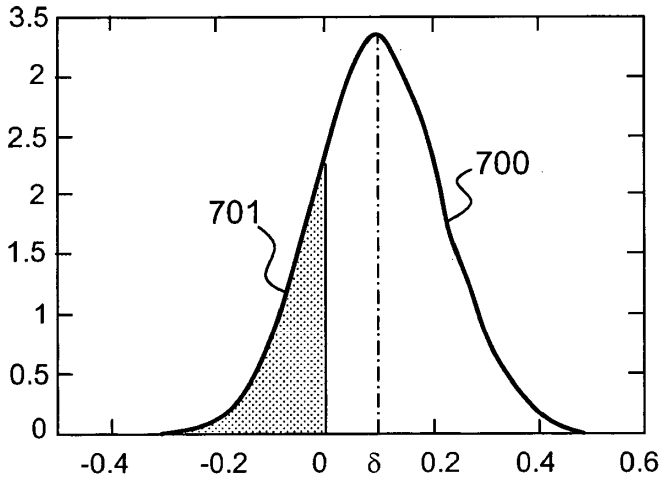
3.5
2
2.5
2
1.5
1
0.5
0
-0.4
-0.2
0
δ
0.2
0.4
0.6
700
701

FIG.7

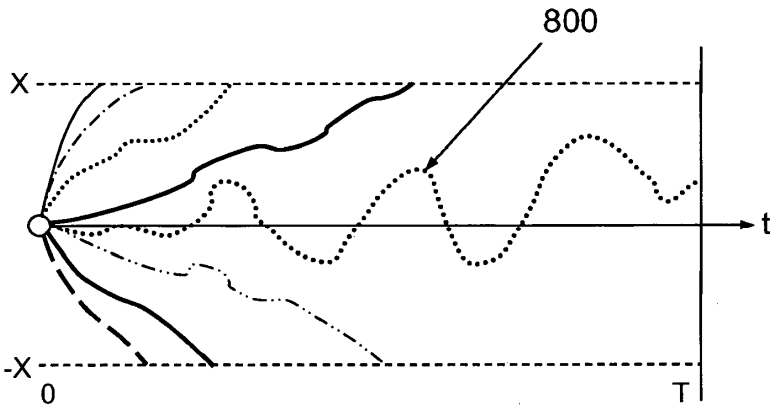

FIG.8

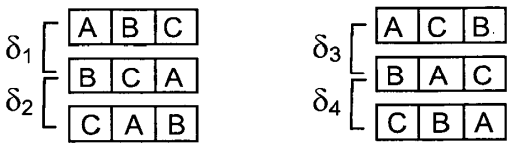

FIG.9

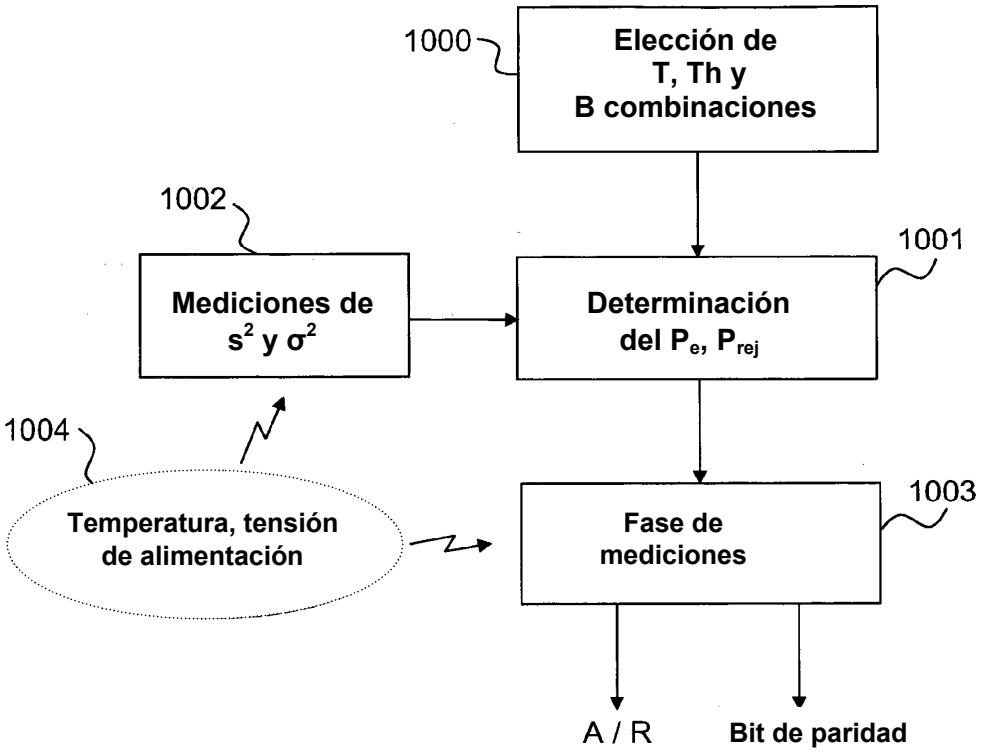
1000
Elección de T, Th y B combinaciones
1002
Mediciones de s^2 y σ^2
1001
Determinación del P_e, P_{rej}
1004
Temperatura, tensión de alimentación
1003
Fase de mediciones
A / R
Bit de paridad

FIG.10

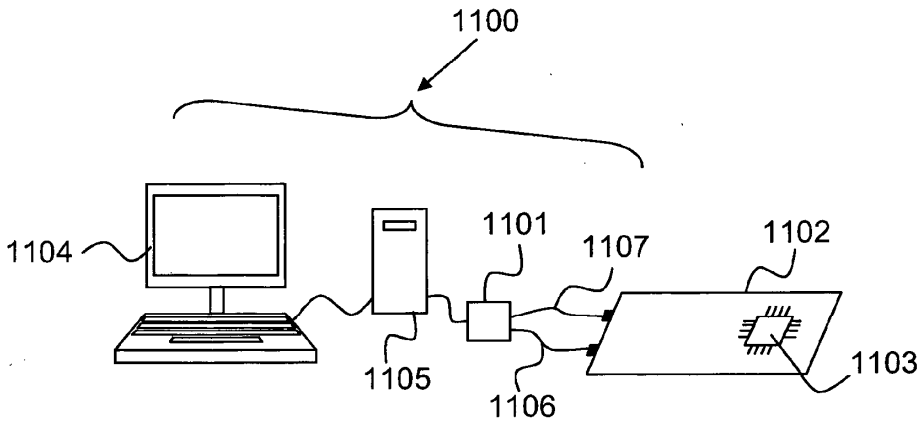
1100
1104
1101
1107
1102
1103
1105
1106

FIG.11