(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 584 527**

(51) Int. CI.:

G11C 7/04 (2006.01)
G11C 7/10 (2006.01)
G11C 7/20 (2006.01)
G11C 11/412 (2006.01)
H03K 3/037 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.04.2009 E 09732238 (2)**

(97) Fecha y número de publicación de la concesión europea: **11.05.2016 EP 2269133**

(54) Título: **Método para reducir la aparición de quemado debido a inestabilidad de temperatura en polarización negativa**

(30) Prioridad:

17.04.2008 EP 08154744

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.09.2016

(73) Titular/es:

INTRINSIC ID B.V. (50.0%)
High Tech Campus 9
5656 AE Eindhoven, NL y
NXP B.V. (50.0%)

(72) Inventor/es:

TUYLS, PIM, THEO;
SCHRIJEN, GEERT, JAN y
KRUSEMAN, ABRAHAM, C.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método para reducir la aparición de quemado debido a inestabilidad de temperatura en polarización negativa

La invención se refiere a una técnica para reducir el quemado producido por inestabilidad de temperatura en polarización negativa (NBTI, del inglés "Negative Bias Temperature Instability") en un dispositivo, particularmente para su uso en un dispositivo que usa una función físicamente inclonable (PUF, del inglés "Physically Unclonable Function") con la finalidad de identificación del mismo o con la finalidad de almacenamiento de claves seguras basado en una PUF.

Los dispositivos configurables en campo, tales como las Matrices de Puertas Programables en Campo (FPGA), son ampliamente usados para la realización de prototipos de diseños electrónicos y algoritmos. Adicionalmente, se usan crecientemente como bloques de construcción dedicados en productos de consumo. Su ventaja principal comparados con los ASIC (Circuitos Integrados de Aplicación Específica) es su flexibilidad, dado que pueden configurarse en el campo. Las FPGA se configuran normalmente usando datos, normalmente llamados una corriente de bits de configuración o simplemente corriente de bits, que se suministra al dispositivo después de que el dispositivo se integre en una aplicación. Un tipo popular de FPGA es la FPGA basada en SRAM. Este tipo de chip FPGA solo tiene memoria volátil integrada y por ello pierde su configuración cuando la alimentación se desconecta. Con la alimentación (o "arranque"), la FPGA se configura por medio de una corriente de bits que se carga desde una memoria no volátil externa (por ejemplo una memoria solo de lectura programable (PROM), flash, etc.).

Se pierden beneficios significativos debido a problemas tales como el clonado de dispositivos basándose en los CI y/o sobre-producción no notificada de los mismos. De ese modo, es altamente deseable tener la capacidad de identificar de modo único un dispositivo particular y/o impedir la configuración del mismo con datos de configuración no autorizados. Una forma conocida para identificar de modo único un dispositivo programable en campo es el uso de una función físicamente inclonable (PUF). Las PUF son esencialmente funciones aleatorias ligadas a un dispositivo físico de tal manera que es computacionalmente imposible predecir el resultado de la función sin evaluarla realmente usando el dispositivo físico. Dado que una PUF no puede copiarse o modelizarse, un dispositivo equipado con una PUF se convierte en inclonable (véase, por ejemplo, 1) P. Tuyls, G. J. Schrijen, B. Skoric, J. van Geloven, N. Verhaegh, R. Walters, "Read-proof hardware from protective coatings", L. Goubin y M. Matsuit, Editors Proceedings of Cryptographic Hardware and Embedded Systems 2006, volumen 4249 de LNCS, páginas 369-383, Springer 2006; o 2) J. Guajardo, S. S. Kumar, G. J. Schrijen, P Tuyls, "FPGA intrinsic PUFs and their use for IP protection", P. Paillier y I. Verbauwhede, Editors Proceedings of Cryptographic Hardware and Embedded Systems Conference (CHES) 2007, volumen 4727 de LNCS, páginas 63-80, Springer 2007).

Un ejemplo conocido de una PUF usada para identificar de modo único un dispositivo es la denominada PUF de SRAM, que se basa en el hecho de que, cuando se inicia una célula SRAM, se inicia en un estado aleatorio debido a variaciones en los voltajes de umbral de los transistores (que, a su vez, son debidas a variaciones en el dopado). Cuando esto se realiza múltiples veces, cada celda se iniciará en el mismo estado la mayor parte de las veces.

Realmente, la invención puede usarse para cualquier tipo de elemento de memoria que se base en un bucle de realimentación en el que se usen los transistores que experimentan la NBTI, y que sean susceptibles a parámetros de producción de modo que muestren el comportamiento de inicio descrito.

Cualquier elemento de memoria que muestre el comportamiento de inicio descrito se denomina como elemento de memoria impugnable, o brevemente un elemento de memoria, en la presente solicitud. Ejemplos de dichas celdas de memoria son las celdas de memoria SRAM tal como se ha mencionado anteriormente, aunque también otras celdas de memoria basadas en cerrojos de acoplamiento cruzado, por ejemplo las PUF mariposa tal como se describen en la solicitud de patente europea EP07114732.6 y elementos de memoria tales como biestables.

En referencia a la Figura 1 de los dibujos, una celda SRAM comprende dos inversores en acoplamiento cruzado 1, 2 con conexiones externas a través de dos transistores adicionales (no mostrados). Cada uno de los inversores 1, 2 comprende dos transistores, siendo uno de los transistores un transistor p-MOS y siendo el otro un transistor n-MOS. Como es bien conocido para un experto en la materia, para llevar un transistor p-MOS al estado de conducción, la tensión puerta-fuente aplicada al transistor debe ser más pequeña que la tensión de umbral V_T del transistor. Para un transistor p-MOS, por lo tanto, cuando la tensión aplicada a la puerta es más baja que la tensión de umbral, el transistor es llevado al estado de conducción. Por el contrario, para un transistor n-MOS, cuando la tensión aplicada a la puerta es más baja que la tensión de umbral, actúa como una resistencia y cuando la tensión aplicada a la puerta es más alta que la tensión de umbral, el transistor n-MOS es llevado al estado de conducción.

El valor de la tensión de umbral V_T se determina principalmente por la cantidad de material de dopado presente en el transistor y, dado que esta cantidad de material de dopado no es constante durante la producción, múltiples transistores tendrán un intervalo de tensiones de umbral diferentes, e incluso aunque se fabricaran en la misma fábrica, e incluso si fueron parte del mismo lote. Esto implica, por lo tanto, que la tensión puerta-fuente que se requiere aplicar a un transistor para llevarle al estado de conducción (o de resistencia) también variará. Por lo tanto, además del hecho de que los valores de inicio de un conjunto particular de células SRAM es probable que sean los

mismos cada vez, los valores de inicio de diferentes celdas SRAM es probable que sean diferentes. Por ello, la respuesta de las celdas al inicio en una disposición de celdas SRAM puede considerarse que es una PUF.

En la práctica, sin embargo, el problema principal que puede surgir es el envejecimiento asimétrico que afecta principalmente a los transistores MOSFET de tipo p en una celda SRAM debido al fenómeno conocido como inestabilidad de temperatura con polarización negativa (NBTI). La NBTI provoca la generación de trampas de interfaz bajo condiciones de polarización negativa ($V_{gs} = -V_{dd}$) en transistores pMOS, y de ese modo provoca que la tensión de umbral del mismo disminuya. Como resultado, el comportamiento de inicio preferido de las celdas SRAM afectadas cambia a lo largo del tiempo y, por lo tanto, afectará adversamente a la fiabilidad de la respuesta PUF de las celdas SRAM. Esta degradación de los dispositivos pMOS debido a la NBTI es conocido como quemado.

Como se ha dicho anteriormente algunos de los otros elementos de memoria que son susceptibles al envejecimiento y tienen propiedades similares a una PUF son los anteriormente mencionados PUF y biestables de mariposa y todos los otros elementos de memoria basados en biestables o cerrojos de acoplamiento cruzado.

El documento de S.V. Kumar, Ch.H. Kim, S.S.Sapatnekar, "Impact on SRAM Read Stability and Design for Reliability", Proceedings of the 7th International Symposium on Quality Electronic Design, págs. 210-218, 2006, describe un método para la recuperación del margen de ruido estático de una celda SRAM mediante el basculamiento periódico del contenido de datos de la célula. Sin embargo, este proceso funciona basado en que la celda será alimentada durante largos periodos de tiempo y, si la técnica se implementa por software, hay una sobrecarga de tiempo que hace impráctico su uso con grandes matrices de memoria, mientras que si la técnica se implementa en hardware, hay obviamente una sobrecarga significativa en coste y tamaño. Esta técnica provoca que ambos transistores pMOS de una celda SRAM se envejezcan más simétricamente, pero no es ideal para preservar el comportamiento de inicio de las celdas SRAM.

Es un objetivo de la presente invención proporcionar un método para reducir el impacto de la Inestabilidad de Temperatura con Polarización Negativa en el comportamiento de inicio de un elemento de memoria usado en un circuito integrado para una respuesta de PUF.

De acuerdo con la presente invención, se proporciona un método de acuerdo con la reivindicación 1.

De acuerdo con este método, la polarización negativa aplicada a los elementos de memoria como resultado del proceso de inicio se reduce antes de que tenga lugar una degradación temporal significativa del rendimiento de los transistores p-MOS de los elementos de memoria. Al mantener un patrón de respuesta inversa en la memoria, aunque habrá alguna degradación del dispositivo debido a que aún se aplicará una cierta polarización negativa a los transistores p-MOS del elemento de memoria, dicha degradación (o "envejecimiento") se consigue de tal manera que se estabilicen los valores de inicio de los elementos de memoria, mejorando de modo efectivo el comportamiento de inicio de los elementos de memoria.

En una realización a modo de ejemplo de la presente invención, el patrón de datos puede, para cada proceso de inicio, ser el inverso a un patrón de respuesta generado durante ese proceso de inicio respectivo.

Preferentemente, los datos de respuesta de inscripción se encriptan con una clave. La clave con la que se encriptan los datos de inscripción puede ocultarse en el dispositivo o, en el caso de una FPGA, en la corriente de bits de configuración de la FPGA.

Sin embargo, en una realización más preferida, el patrón de datos es la inversa del patrón de respuesta obtenido durante una fase de inscripción. Se ha determinado que usando la inversa de un patrón de respuesta obtenido durante una fase de inscripción se consigue un mejor resultado anti-envejecimiento que con el uso de la inversa de un patrón de respuesta de la fase de inicio respectiva. En este caso, la fase de inscripción se realiza preferentemente por el fabricante en el momento de la producción o en un momento posterior por unos terceros de confianza.

En una aplicación preferida, el dispositivo puede comprender una matriz de puertas programable en campo (FPGA), en cuyo caso, los elementos de memoria comprenden celdas de memoria SRAM y el patrón de datos, que es preferentemente el patrón de respuesta determinado durante la fase de inscripción o los datos de ayuda a partir de los que puede reconstruirse el patrón de respuesta, se almacenan beneficiosamente (en una forma protegida, por ejemplo cifrados o en la forma de datos de ayuda) a continuación de la corriente de bits de configuración o programa que se ejecutará en el chip en una memoria externa (o parcheado dentro de la corriente de bits), que puede ser una memoria no volátil proporcionada sobre la misma tarjeta de circuito impreso en la que se localiza la FPGA.

También de acuerdo con la presente invención, se proporciona un dispositivo electrónico para la implementación del método de acuerdo con la reivindicación 1.

En una realización a modo de ejemplo, el componente electrónico puede comprender una FPGA que comprende una matriz de celdas SRAM y los medios de almacenamiento pueden comprender una memoria no volátil

incorporada en o cerca del dispositivo. Alternativamente, sin embargo, el componente puede comprender un ASIC con celdas de memoria SRAM como elementos de memoria y memoria no volátil integrada, o una tarjeta inteligente con las mismas propiedades.

En una realización adicional de la presente invención en la que la memoria es parte de una FPGA, se proporciona un dispositivo de almacenamiento electrónico para un componente electrónico tal como se ha definido anteriormente, en el que se almacena un patrón de datos para aplicación a al menos los elementos de memoria en los que está contenido el primer patrón de respuesta de los valores de inicio, en el que preferentemente el patrón de datos en la inversa de una respuesta determinada durante la fase de inscripción.

Adicionalmente se proporciona un producto de programa informático que comprende instrucciones ejecutables por un procesador que, cuando se cargan y ejecutan en el procesador implementan el método de acuerdo con la reivindicación 1.

Aún más, se proporciona un producto de programa informático que comprende datos de configuración, preferentemente en la forma de una corriente de bits, que, cuando se cargan sobre un circuito electrónico configurable, configuran el circuito electrónico para realizar el método de acuerdo con la reivindicación 1.

Para evitar dudas, una fase de inscripción es cualquier proceso de inicio durante el que se mide una respuesta con respecto al dispositivo y a partir de la que se extrae una clave o "identificador" por primera vez (siendo interpretable "primera vez" relativamente, es decir, como la primera vez dentro de una sesión de inscripción y autentificaciones). Un patrón de datos son los datos leídos desde los elementos de memoria como resultado del proceso de inicio, tanto si es una fase de inscripción como si es una fase de verificación. Es posible usar todos los elementos de memoria del dispositivo para generar el identificador y, posteriormente, el patrón de respuesta para su uso durante la fase de verificación. Sin embargo, debido a que el primer patrón de respuesta necesita ser escrito de nuevo en todas las celdas usadas en esta forma, es deseable minimizar la cantidad de elementos que se usan en esta forma, y es deseable minimizar la cantidad de elementos que se usan en esta forma, se prefiere usar justamente un subconjunto de elementos de memoria para esta finalidad. Se apreciará por lo tanto que el identificador para un dispositivo puede cambiarse simplemente mediante el cambio del subconjunto de elementos de memoria elegidos a partir de los que se leen los datos de inicio durante la fase de inscripción y/o se puede definir más de un identificador para un dispositivo mediante la generación de dos o más identificadores usando dos o más subconjuntos respectivos de elementos de memoria.

Estos y otros aspectos de la presente invención serán evidentes a partir de, y clarificados con referencia a, las realizaciones descritas en el presente documento.

Por exhaustividad se menciona que la solicitud de patente internacional, con número de publicación WO/2006/053304 y título "VOLATILE DEVICE KEYS AND APPLICATIONS THEREOF" desvela una clave determinada a partir de una respuesta volátil usando circuitos sobre un dispositivo.

Por exhaustividad se referencian los artículos "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags", por Holcomb, et ál. "Impact of NBTI on SRAM read stability and design for reliability", por Kumar, et ál.

Se describirán ahora realizaciones de la presente invención a modo de ejemplos solamente y con referencia a los dibujos adjuntos, los que:

La Fig. 1 es una ilustración parcial esquemática de una celda SRAM;
la Fig. 2 es un diagrama de flujo esquemático que ilustra las etapas principales en un proceso de inicio de acuerdo con una realización a modo de ejemplo de la presente invención; y
la Fig. 3 ilustra gráficamente las distancias de Hamming entre valores de inicio de una medición de inscripción y mediciones en instancias posteriores de tiempo obtenidas por experimentación con respecto a una realización a modo de ejemplo de la presente invención. Se muestran tres situaciones: "valores de inicio frescos" se refiere a la situación en la que, después de cada medición de inicio, se mantienen en memoria los últimos valores de inicio, "valores de inicio frescos invertidos" que se refiere a la situación en la que, después de la medición de los valores de inicio se escriben de nuevo en las celdas de memoria SRAM la inversa de estos valores, "valores de inicio dorados invertidos" se refiere a la situación en la que se escriben de nuevo los inversos de los valores de inicio medidos durante la fase de inscripción después de cada medición de inicio.

Por exhaustividad, y volviendo a hacer referencia a la Figura 1 de los dibujos, una celda SRAM comprende dos inversores en acoplamiento cruzado 1, 2 con conexiones externas a través de dos transistores adicionales (no mostrados). Cada uno de los inversores 1, 2 comprende dos transistores, siendo uno de los transistores un transistor p-MOS y siendo el otro un transistor n-MOS. Como es bien conocido para un experto en la materia, para llevar un transistor p-MOS al estado de conducción, la tensión puerta-fuente aplicada al transistor debe ser más pequeña que la tensión de umbral V_T del transistor. Para un transistor p-MOS, por lo tanto, cuando la tensión aplicada a la puerta es más baja que la tensión de umbral, el transistor es llevado al estado de conducción. Por el contrario, para un

transistor n-MOS, cuando la tensión aplicada a la puerta es más baja que la tensión de umbral, actúa como una resistencia y cuando la tensión aplicada a la puerta es más alta que la tensión de umbral, el transistor n-MOS es llevado al estado de conducción.

Si la tensión de alimentación sobre la SRAM es cero, los dos transistores pMOS de la celda SRAM están en estado de conducción y los dos transistores nMOS están en estado de no conducción. Cuando la tensión sobre la celda SRAM comienza a incrementarse (en el inicio), las tensiones sobre las puertas de los dos transistores pMOS comienzan a incrementarse en consecuencia. Supongamos, por ejemplo, que $V_{1T} < V_{2T}$. En este caso, la tensión en elevación sobre la celda SRAM afectará primero al $pMOS_1$ y posteriormente (según la tensión a través de la celda SRAM continúa elevándose) al $pMOS_2$. Como resultado, se lleva primero al $pMOS_1$ a un estado de no conducción, de modo que la salida del inversor 1 es baja y la del inversor 2 es alta y la celda SRAM contiene un "0". Si, por otro lado, $V_{2T} < V_{1T}$, la celda SRAM contendría un "1" en el inicio. Así, el comportamiento de inicio de una celda SRAM depende de las relaciones entre los pares de tensiones de umbral V_{1T} y V_{2T} de las celdas SRAM respectivas y estas relaciones se distribuirán sustancialmente de modo aleatorio a través de la matriz de celdas debido a las concentraciones de dopado anteriormente mencionadas. Es este hecho, en conexión con el hecho de que la respuesta de la matriz de celdas SRAM durante un cierto número de eventos de inicio es probable que sea el mismo cada vez, el que ha dado como resultado el uso del patrón de respuesta de cada matriz SRAM como una PUF.

En la práctica, sin embargo, el problema principal que puede surgir es el envejecimiento asimétrico que afecta principalmente a los transistores MOSFET de tipo p en una celda SRAM debido al fenómeno conocido como Inestabilidad de Temperatura con Polarización Negativa (NBTI). La NBTI provoca la generación de trampas de interfaz bajo condiciones de polarización negativa ($V_{gs} = -V_{dd}$) a temperaturas elevadas en los transistores pMOS, y de ese modo provoca que la tensión de umbral del mismo disminuya. Como resultado, el comportamiento de inicio preferente de las celdas SRAM afectadas cambia a lo largo del tiempo y, por lo tanto, afectará adversamente a la fiabilidad de la respuesta PUF de la FPGA. Esta degradación de los dispositivos pMOS debido a la NBTI es conocido como quemado.

Considérese la situación en la que el estado de inicio preferente de una celda SRAM es "1" (es decir, por el ejemplo dado anteriormente, $V_{2T} < V_{1T}$). Si el valor del dato de configuración escrito posteriormente es también "1", en otras palabras, si se mantiene el valor "1" en la memoria durante un período de tiempo más largo (más allá del inicio), existirá una polarización negativa (es decir $V_{1gs} = -V_{dd}$) sobre el transistor pMOS del inversor 1. Como se ha explicado anteriormente, la NBTI provocará que V_{1T} disminuya a lo largo del tiempo. De ese modo, en algún punto, V_{1T} disminuirá hasta el punto de que $V_{2T} > V_{1T}$. Esto significa que el comportamiento de inicio de la celda SRAM habrá cambiado respecto al comportamiento de inicio preferente de modo que, cuando se inicia, contendrá ahora un "0" en lugar de un "1". Por otro lado, cuando se escribe un "0" en la celda SRAM, existirá una polarización negativa (es decir $V_{2gs} = -V_{dd}$) sobre el transistor pMOS del inversor 2. Por ello, la NBTI provocará, en este caso, que V_{2T} disminuya y la diferencia entre V_{1T} y V_{2T} se incrementará adicionalmente, de modo que el estado de inicio cero preferente de la celda SRAM se convertirá en más pronunciado.

De acuerdo con la presente invención, se propone atenuar el impacto de la NBTI sobre el estado de inicio preferente de las celdas SRAM escribiendo la inversa de un patrón de respuesta a la matriz de celdas SRAM después de que se haya medido el patrón de respuesta inicial. Se proporciona en la figura 2 de los dibujos un diagrama de flujo que ilustra las etapas principales de un proceso de inicio completo de acuerdo con la invención.

La NBTI es un mecanismo claramente lento y se ha documentado que la cantidad de degradación en Margen de Ruido Estático (SNM) es notable solo después de que se haya aplicado continuamente una polarización negativa durante 10^5 segundos (~1,16 días). Por lo tanto, si el contenido de las celdas se bascula prontamente después del inicio (lo que puede suponerse que ocurre al menos una vez al día), entonces puede mantenerse la mayor parte, si no todo, el comportamiento de los transistores pMOS.

En una realización a modo de ejemplo de la presente invención, la "contramedida" aplicada a la matriz de celdas SRAM después del inicio puede comprender la inversa del patrón de respuesta determinado durante ese proceso de inicio particular. En este caso, el patrón de respuesta determinado se escribiría en la memoria no volátil de la FPGA, se aplicaría una función inversa al mismo y el patrón de respuesta inversa así creado se aplicaría posteriormente como una entrada a la matriz SRAM.

Sin embargo, en una realización alternativa, más preferida, la "contramedida" (es decir "segundo patrón de respuesta") aplicada a la matriz de celdas SRAM después del inicio comprende la inversa de un patrón de respuesta determinado durante la fase de inscripción (realizada por el fabricante en el momento de la producción o en un momento posterior por un tercero de confianza). Esto no solo reduce la cantidad de procesamiento que se requiere realizar (debido a que la inversa del patrón de respuesta original puede generarse durante la fase de inscripción y almacenarse en la memoria no volátil de la FPGA a todo lo largo de su vida, en lugar de tener que proporcionar medios para conseguir la funcionalidad inversa en cada proceso de inicio), sino que los inventores han determinado también que esto mejora la fiabilidad de la PUF, como se ilustra gráficamente en la Figura 3 de los dibujos, en la que los valores de "inicio dorado" invertido se refieren a la respuesta del patrón de respuesta medido durante la fase de inscripción, valores que se almacenan en la memoria no volátil del dispositivo durante el envejecimiento del mismo.

Se apreciará que, aunque la presente invención se ha descrito anteriormente específicamente en relación a una FPGA, la presente invención puede aplicarse igualmente a otros tipos de circuitos integrados sobre los que se construyen identificadores intrínsecos de verificación y claves seguras (por ejemplo, microcontroladores DSP, ASIC, CI de tarjetas inteligentes, etc.).

Debería tomarse nota también de que las realizaciones anteriormente mencionadas ilustran en lugar de limitar la invención, y que los expertos en la materia serán capaces de diseñar muchas realizaciones alternativas sin apartarse del alcance de la invención tal como se define por las reivindicaciones adjuntas. En las reivindicaciones, cualesquiera signos de referencia colocados entre paréntesis no deben ser interpretados como limitativos de las reivindicaciones. La palabra "comprendiendo" y "comprende", y similares, no excluyen la presencia de elementos o etapas distintos de aquellos listados en cualquier reivindicación o en la memoria descriptiva como un conjunto. La referencia singular de un elemento no excluye la referencia plural de dichos elementos y viceversa. La invención puede implementarse por medios de hardware que comprenden diversos elementos distintos, y por medio de un ordenador adecuadamente programado. En una reivindicación de dispositivo que enumere diversos medios, varios de estos medios pueden realizarse mediante uno y el mismo artículo de hardware. El mero hecho de que ciertas medidas se enumeren en reivindicaciones dependientes mutuamente diferentes no indica que no pueda usarse como ventaja una combinación de estas medidas.

REIVINDICACIONES

1. Un método para atenuar el efecto de quemado y permitir la realización de un proceso de inicio con respecto a un dispositivo que comprende una pluralidad de elementos de memoria que pueden cambiarse, en donde los elementos de memoria tienen la capacidad de, tras el inicio, generar un patrón de respuesta de valores de inicio útiles para la identificación dado que el patrón de respuesta depende de características físicas de los elementos de memoria, comprendiendo los elementos de memoria un bucle de realimentación que usa transistores, el método **caracterizado por** la etapa de, tras el inicio de los elementos de memoria, escritura de un patrón de datos en los elementos de memoria que es el inverso a un patrón de respuesta que se leyó previamente desde los mismos elementos de memoria, en donde la escritura del patrón de datos en los elementos de memoria que es el inverso al patrón de respuesta que se leyó previamente desde los mismos elementos de memoria es parte de un proceso de inicio y se prosigue después del inicio y de la medición de un patrón de respuesta inicial.

2. Un método de acuerdo con la reivindicación 1 en el que el patrón de datos que se escribe es, para cada proceso de inicio, inverso al patrón de respuesta generado como resultado de ese proceso de inicio respectivo.

3. Un método de acuerdo con la reivindicación 1, en el que el patrón de datos que se escribe es fijo e inverso al patrón de respuesta generado durante la fase de inscripción.

4. Un método de acuerdo con la reivindicación 3 en el que la respuesta determinada durante la fase de inscripción se almacena en una memoria no volátil, que puede incorporarse al propio dispositivo.

5. Un método de acuerdo con la reivindicación 3, en el que dicha respuesta se almacena en una forma protegida.

6. Un método de acuerdo con la reivindicación 3, en el que los datos de respuesta se encriptan con una clave.

7. Un método de acuerdo con la reivindicación 5, en el que los datos de respuesta se reconstruyen a partir de datos de ayuda.

8. Un método de acuerdo con la reivindicación 1, en el que los elementos de memoria están basados en cerrojos de acoplamiento cruzado.

9. Un método de acuerdo con la reivindicación 1, en el que los elementos de memoria son celdas de memoria SRAM.

10. Un método de acuerdo con la reivindicación 1, en el que los elementos de memoria son biestables.

11. Un método de acuerdo con una cualquiera de las reivindicaciones 1, 3 y 5 en el que el dispositivo comprende una Matriz de Puertas Programable en Campo (FPGA) y los elementos de memoria comprenden celdas de memoria SRAM.

12. Un método de acuerdo con las reivindicaciones 3 y 11, en el que los datos de ayuda, a partir de los que puede reconstruirse el patrón de respuesta determinado durante la fase de inscripción, se almacenan en una memoria externa próxima a la corriente de bits de configuración o al programa que se ejecutará en la FPGA.

13. Un método de acuerdo con la reivindicación 12, en el que la memoria externa es una memoria no volátil proporcionada sobre la misma tarjeta de circuito impreso en la está situada la FPGA.

14. Un producto de programa informático que comprende instrucciones ejecutables por procesador que, cuando se cargan y ejecutan en el procesador, están dispuestas para implementar el método de acuerdo con la reivindicación 1.

15. Producto de programa informático que comprende datos de configuración, preferentemente en la forma de una corriente de bits, que, cuando se cargan en un circuito electrónico configurable, configuran el circuito electrónico para disponerse para la realización del método de acuerdo con la reivindicación 1.

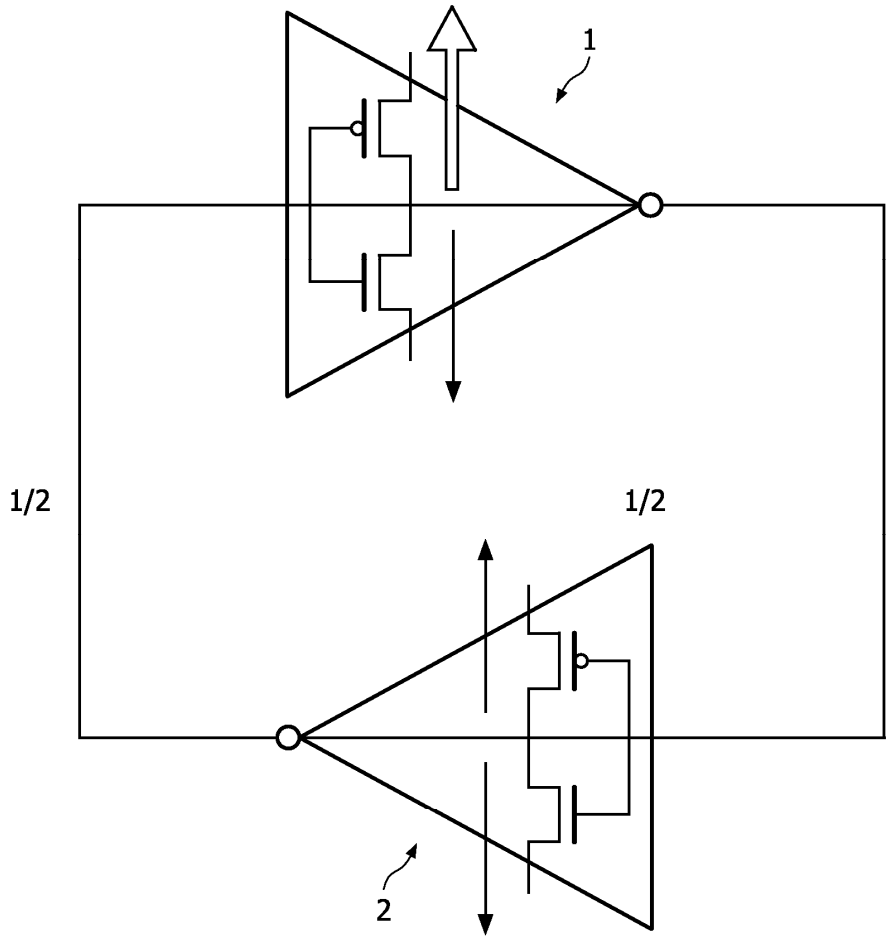

FIG. 1

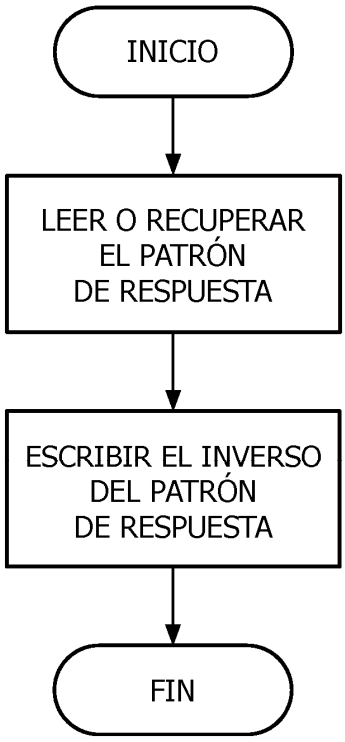
INICIO
LEER O RECUPERAR EL PATRÓN DE RESPUESTA
ESCRIBIR EL INVERSO DEL PATRÓN DE RESPUESTA
FIN

FIG. 2

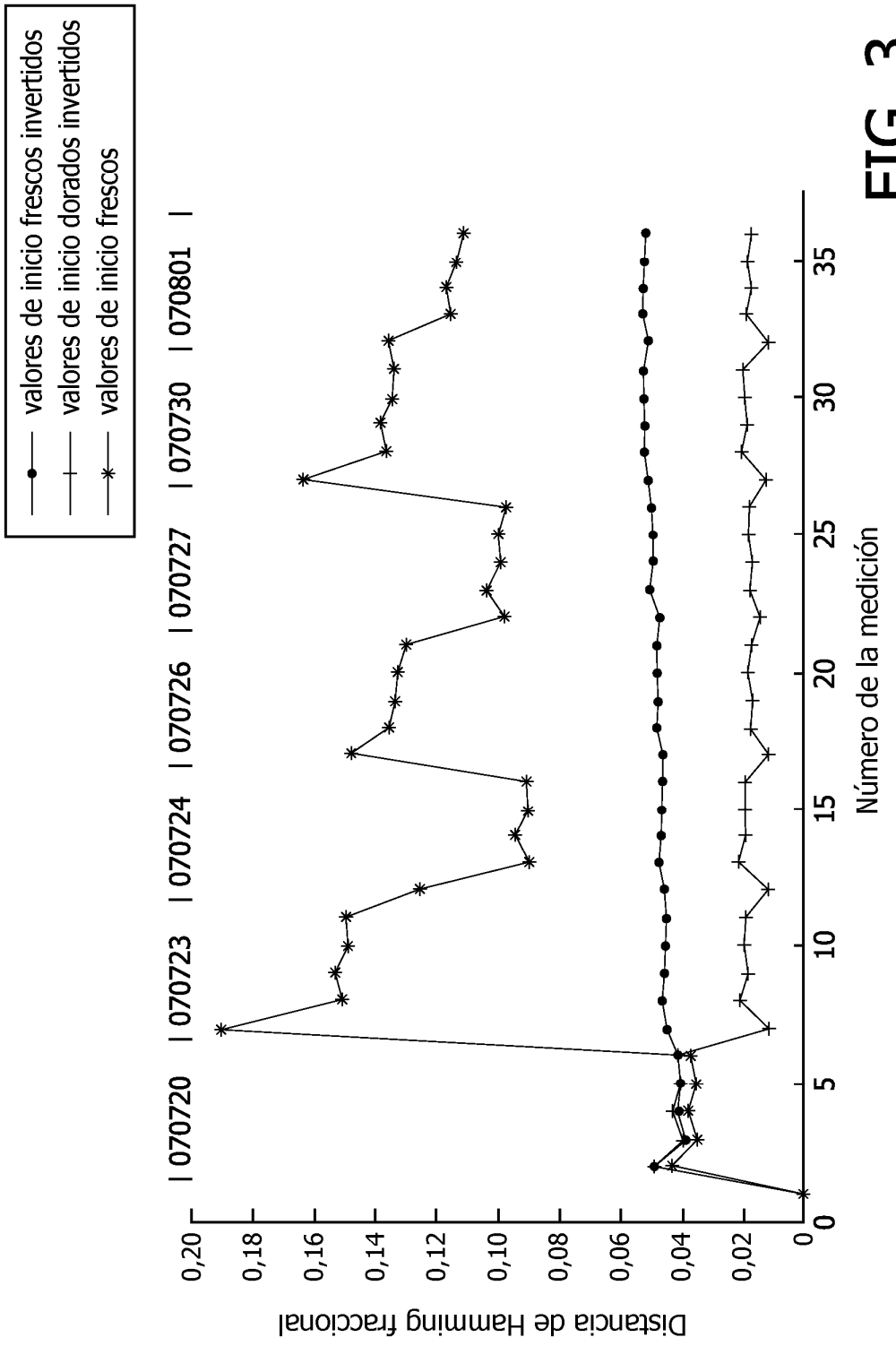
valores de inicio frescos invertidos
valores de inicio dorados invertidos
valores de inicio frescos
070720
070723
070724
070726
070727
070730
070801
Distancia de Hamming fraccional
0,20
0,18
0,16
0,14
0,12
0,10
0,08
0,06
0,04
0,02
0
0
5
10
15
20
25
30
35
Número de la medición

FIG. 3