

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 957 893**

21 Número de solicitud: 202230569

51 Int. Cl.:

G06F 7/58 (2006.01)

12

SOLICITUD DE PATENTE

A1

22 Fecha de presentación:

24.06.2022

43 Fecha de publicación de la solicitud:

29.01.2024

71 Solicitantes:

**CONSEJO SUPERIOR DE INVESTIGACIONES
CIENTÍFICAS (CSIC) (50.0%)**

Av. Marisa Luisa s/n - Pabellón de Perú

41013 Sevilla (Sevilla) ES y

UNIVERSIDAD DE SEVILLA (50.0%)

72 Inventor/es:

ROCA MORENO, Elisenda;

CASTRO LÓPEZ, Rafael;

SARAZÁ CANFLANCA, Pablo y

FERNÁNDEZ FERNÁNDEZ, Francisco Vidal

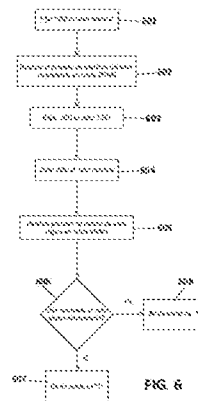
74 Agente/Representante:

PONS ARIÑO, Ángel

54 Título: **MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN DE NÚMEROS VERDADERAMENTE ALEATORIOS**

57 Resumen:

Método para generación de números verdaderamente aleatorios mediante el uso de celdas SRAM que comprende: obtener una tensión de retención de datos (DRV) y un valor lógico preferido para cada celda; conectar la tensión de alimentación de la celda a un valor nominal; escribir un valor lógico no preferido; reducir la tensión de alimentación al valor DRV; aumentar la tensión de alimentación hasta el valor nominal; leer el contenido de la celda de modo que, si se ha mantenido el valor lógico no preferido, se interpreta como un valor lógico; y si ha cambiado, se interpreta como el contrario, permitiendo utilizar todas las celdas como generadores de números aleatorios, aumentando la entropía mínima y realizando la lectura a tensión de alimentación nominal. La invención comprende también un dispositivo con una o más celdas SRAM, al menos una fuente de alimentación; y al menos un procesador configurado para implementar el método.



ES 2 957 893 A1

DESCRIPCIÓN

**MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN DE NÚMEROS
VERDADERAMENTE ALEATORIOS**

5

OBJETO DE LA INVENCION

La invención tiene su aplicación dentro de la industria de la tecnología electrónica, la seguridad y privacidad, la criptografía, los juegos, las telecomunicaciones y el muestreo estadístico.

10

La presente invención tiene por objeto un método y dispositivo asociado para la generación de números verdaderamente aleatorios (TRNG del inglés True Random Number Generation) a partir de celdas de memoria estática de acceso aleatorio (SRAM del inglés Static Random Access Memory) de cualquier característica, es decir, independientemente de que las celdas consideradas tengan un mayor o menor sesgo hacia uno de los valores lógicos.

15

ANTECEDENTES DE LA INVENCION

20

La generación de números verdaderamente aleatorios está normalmente basada en algún proceso físico aleatorio que se utiliza como fuente de entropía, tal como el movimiento browniano, la desintegración nuclear, o, más frecuentemente, el ruido térmico.

25

Para la explotación de dicho ruido térmico, por ejemplo, se pueden emplear diferentes técnicas, como la influencia en el jitter (fluctuación del retraso) de osciladores en anillo o la meta-estabilidad de estructuras CMOS acopladas. En algunas propuestas, se polarizan las estructuras en el punto meta-estable y se dejan evolucionar hacia un estado estable (valor lógico "0" o valor lógico "1) determinado por el ruido. Fijar adecuadamente el punto meta-estable no es un proceso sencillo, por lo que una propuesta popular es usar el proceso de encendido de celdas SRAM.

30

Las celdas SRAM permiten almacenar un bit de información ya que las mismas poseen dos estados estables, uno de los cuales se asocia a un valor lógico "0" y el otro a un valor lógico "1".

35

A efectos ilustrativos, se puede considerar la celda SRAM convencional, representada en la Fig. 1, que está constituida por 6 transistores. Cada una de estas celdas tiene un núcleo formado por dos inversores cruzados (M_1 - M_2 - M_3 - M_4) que permite dos estados lógicos posibles: "0" lógico, correspondiente a que el nodo Q está a una tensión alta y \bar{Q} a una tensión baja, y "1" lógico para la situación inversa. Se puede acceder externamente al núcleo para leer el valor almacenado o para escribir un nuevo valor al habilitar los dos transistores de acceso (M_5 y M_6).

En la operación estándar de una celda SRAM, se realiza un proceso de escritura de un valor lógico ("0" o "1") con la celda polarizada a su tensión de alimentación nominal. Dicho dato queda almacenado de forma indefinida mientras no se interrumpa la alimentación y puede ser leído en cualquier momento a través de los transistores de acceso.

Si las celdas son completamente simétricas, es decir, la mitad derecha de la celda (M_3 - M_4 - M_6) es geométrica y eléctricamente idéntica a la mitad izquierda (M_1 - M_2 - M_5), al realizar el proceso de encendido (es decir, al aumentar la tensión de alimentación desde 0 voltios a su valor nominal sin escribir ningún dato), la celda evolucionaría hacia un estado meta-estable, con igual tensión en sus nodos Q y \bar{Q} . La inevitable presencia de ruido, no obstante, hace que la celda evolucione hacia uno de sus estados estables al final de dicho proceso de encendido ("0" o "1"). En principio, bajo la suposición de total simetría, la celda evolucionaría indistintamente hacia uno u otro nivel lógico cuando su tensión de alimentación creciera a su nivel nominal. Es decir, en una celda existe una probabilidad finita p_0 de que la celda vaya a un "0" lógico, y una probabilidad finita $p_1 = 1 - p_0$ que la celda vaya a un "1" lógico, y si la celda es simétrica p_0 sería igual a p_1 , lo cual resulta ideal para la generación de números verdaderamente aleatorios.

Es esta la filosofía subyacente en la mayoría de las soluciones de la técnica para generar números verdaderamente aleatorios usando celdas SRAM.

Sin embargo, la inevitable presencia de la variabilidad en los procesos de fabricación va a hacer que no exista la celda totalmente simétrica, y, en consecuencia, las celdas van a tener un sesgo más o menos intenso hacia un valor preferido, el "0" o el "1", en distintos procesos de encendido. Que una celda evolucione consistentemente al mismo valor va en contra de la misma esencia de generación de TRN. Solo un porcentaje reducido de

celdas tienen una asimetría entre sus inversores lo suficientemente pequeña como para que este sesgo sea débil y, por consiguiente, su respuesta al encendido se considera inestable, es decir, en distintos encendidos, estas celdas evolucionan a veces al "0" y otras al "1". Dicha asimetría disminuye en gran medida la aleatoriedad que se puede extraer de un conjunto de celdas SRAM. Esto puede no ser un gran problema cuando se considera una SRAM muy grande, donde hay muchas celdas para elegir. Sin embargo, si el TRNG se integrase en otro sistema que ya dispone de un número de celdas SRAM, pero este número fuera insuficiente para implementar dicho TRNG, la inclusión de las celdas adicionales necesarias llevaría a un sobre coste de área no deseado.

En muchos casos, se utiliza una matriz de celdas SRAM para generar una cadena de bits cuando se conecta la tensión de alimentación sin escribir previamente ningún dato (proceso de encendido). Para generar números verdaderamente aleatorios (TRN) a partir de ellas, se utiliza un algoritmo de acondicionamiento que condensa una larga cadena de bits en otra cadena más corta y de longitud fija. La cantidad de compresión requerida depende de la entropía mínima en los bits de entrada.

Sin embargo, este procedimiento se encuentra con crecientes dificultades, porque las asimetrías suelen aumentar en las tecnologías más modernas por lo que el porcentaje de celdas que evolucionan consistentemente en distintos procesos de encendido hacia un mismo valor lógico es cada vez mayor, lo que las hace inadecuadas para obtener una alta entropía. Por tanto, el número de bits aleatorios que se puede obtener en un proceso de encendido se ve drásticamente reducido. Cuantos más bits sean necesarios porque menor sea la entropía total, más complejo será el procesamiento posterior y, por tanto, más lenta será la generación de números aleatorios.

El hecho de que haya celdas asimétricas y simétricas hace que se haya propuesto utilizar las primeras para identificación/autenticación y las segundas para la generación de números verdaderamente aleatorios. Una técnica posible de clasificación de las celdas es mediante el encendido consecutivo de las mismas un cierto número de veces: si las celdas se encienden siempre al mismo valor se consideran estables y si alguna vez no se encienden al mismo valor, se consideran inestables. Son éstas últimas las que se utilizan para la generación de números aleatorios.

35

Aunque esta aproximación supone un aumento significativo de la entropía del sistema, sufre de ciertos inconvenientes tales como el reducido número de celdas simétricas en tecnologías de escala nanométrica (lo que lleva a necesitar un conjunto mucho mayor de celdas del que poder extraer el reducido subconjunto de celdas simétricas) o los errores de identificación de la inestabilidad al utilizar un número de encendidos relativamente reducido durante el proceso de clasificación de las celdas.

Por ejemplo, en un estudio se obtuvo que alrededor del 90% de un conjunto de celdas se clasificaron como estables (es decir, sin aleatoriedad), y entre las clasificadas como inestables, algunas mostraron un valor diferente de su valor preferido en un porcentaje relativamente bajo del número de encendidos (es decir, muy poca aleatoriedad). Esto significa que se necesitaría una gran cantidad de celdas SRAM para garantizar la correcta generación de aleatoriedad. Además, a medida que las dimensiones mínimas de los nodos tecnológicos se reducen y la variabilidad del proceso se vuelve más acentuada, la asimetría entre el par de inversores de las celdas puede aumentar, lo que conduciría a una mayor reducción de la aleatoriedad en el encendido.

Una aproximación para conseguir una cierta relación preestablecida entre celdas estables (que se pueden explotar como funciones físicamente no clonables (PUF, del inglés Physical Unclonable Function)) y celdas apropiadas para generación de números aleatorios está basada en conseguir un cierto porcentaje de celdas inestables mediante la manipulación de la tensión de alimentación de la celda SRAM.

Para ello, se considera un conjunto de valores de la tensión de alimentación, por ejemplo, tres valores, y se realiza un test de escritura/lectura de "0" lógico y "1" lógico en la matriz de celdas SRAM. Las celdas que pasan los tests para alguna de las tensiones de alimentación, pero no para las otras, son aquellas en las que la tensión V_{min} de la celda (la tensión de alimentación mínima a la que la celda puede operar) está comprendida entre las tres tensiones de alimentación usadas en los tests de escritura/lectura. Estas celdas se consideran inestables, y, por tanto, apropiadas para la generación de números verdaderamente aleatorios. Una vez seleccionadas las celdas para generar un número aleatorio se ejecuta un proceso de encendido de dichas celdas utilizando como tensión de alimentación el valor intermedio de las tres tensiones usadas en el proceso de selección. El valor obtenido en la lectura del contenido de las celdas constituye el número aleatorio.

Sin embargo, este esquema de generación tiene algunos inconvenientes:

- (1) El proceso de selección está relacionado con la tensión V_{min} , que está determinada por errores de escritura, lectura y retención, mientras que el valor de encendido que determina el número aleatorio en sí está principalmente relacionado con errores de retención.
- (2) El proceso de lectura del valor de encendido con una tensión de alimentación cercana a V_{min} puede tener muchas dificultades técnicas y ser propensa a errores.

5

10

En muchos casos, los números verdaderamente aleatorios se emplean como semillas de calidad para algoritmos de generación de números pseudoaleatorios. Estos algoritmos pueden ser no deterministas o deterministas, éstos últimos estando especialmente pensados para sistemas de bajo coste y consumo y baja tasa de bits. Usar el encendido de una SRAM como semilla de un algoritmo de generación de números pseudoaleatorios palió el problema de tener un número limitado de números aleatorios debido al reducido número celdas inestables.

15

En otros casos, se ha propuesto también irradiar las celdas para aumentar la entropía. Las limitaciones en cuanto a coste y equipamiento necesario en este caso son obvias.

20

De la revisión del estado de la técnica se puede concluir que las técnicas existentes sufren de al menos una de las siguientes limitaciones:

- (1) Alto coste puesto que solo un pequeño porcentaje de celdas son potencialmente útiles para generar TRNs.
- (2) Necesidad de postprocesamiento complejo de los bits.
- (3) Necesidad de equipamiento de alto coste, por ejemplo, para irradiar celdas.
- (4) Procesos de selección de celdas no alineados con proceso de encendido.
- (5) Procesos de lectura complejos.

25

30

DESCRIPCIÓN DE LA INVENCION

La invención se refiere a un método para la generación de números verdaderamente aleatorios mediante el uso de celdas SRAM, que permite generar números verdaderamente aleatorios, incluso a partir de celdas que se etiquetarían como estables (es decir, sin aleatoriedad), según el proceso convencional de usar su valor de

35

encendido que se ha explicado en la sección anterior, las cuales son gran mayoría en un conjunto de celdas SRAM.

5 El método objeto de la invención es independiente de la topología de celda SRAM empleada.

10 A diferencia del método de encendido convencional, que solo puede generar números aleatorios verdaderos a partir de una porción muy limitada del número total de celdas en un circuito, el método de la invención se basa en una métrica de tensión de retención de datos (DRV del inglés Data Retention Voltage), y es capaz de extraer aleatoriedad de cualquier celda SRAM.

15 En las celdas de memoria SRAM se conoce como tensión de retención de datos a la menor tensión de alimentación a la cual el dato almacenado se mantiene inalterado. Se define de manera más precisa en el contexto de la invención como el valor de tensión de alimentación en el que, cuando una celda está almacenando su valor no preferido, sufre un cambio (en inglés, bit-flip) hacia su valor preferido.

20 Así, el método de la invención comprende una etapa previa de obtención de la tensión de retención de datos (DRV) y un valor lógico preferido de una celda.

Esta obtención puede llevarse a cabo de múltiples maneras.

25 Preferentemente, esta etapa puede llevarse a cabo definiendo un rango de posibles valores de tensión de retención de datos. Con seguridad dicho rango de valores estará comprendido entre 0 voltios (V) y la tensión de alimentación nominal. El valor de DRV es específico de cada celda, pero en cualquier tecnología es sencillo determinar valores extremos más precisos de dicho DRV mediante simulación o mediante medidas experimentales.

30 Entonces, se escribe un valor "1" lógico, se reduce el valor de tensión de alimentación desde una tensión nominal al valor más alto del rango determinado; se aumenta nuevamente el valor de tensión al valor nominal y se comprueba si ha cambiado el valor lógico almacenado.

35

A continuación, se repite el mismo proceso disminuyendo el valor al que se baja la tensión de alimentación un cierto valor ΔV , hasta o bien detectar un cambio del valor lógico almacenado para un cierto valor de la tensión de alimentación, fijando dicho valor como DRV1; o bien hasta alcanzar el valor inferior del rango determinado, fijando dicho valor inferior como DRV1.

Entonces, se repite el mismo proceso grabando un "0" lógico para determinar la tensión de alimentación DRV0.

Se determina el mayor valor entre DRV0 y DRV1 como valor de DRV de la celda y el correspondiente valor lógico se fija como el valor no preferido de la celda, que es el valor lógico opuesto al valor preferido de la celda.

Una vez disponible la tensión de retención de datos y el valor lógico preferido de la celda, se procede a conectar la celda en un valor de tensión de alimentación nominal y seguidamente, se escribe su valor lógico no preferido en la celda.

Entonces, se baja la tensión de alimentación de la celda a un valor de tensión próximo a la tensión de retención de datos (DRV) y se vuelve a aumentar la tensión hasta el valor de tensión de alimentación nominal para comprobar si se ha mantenido el valor lógico no preferido.

Si se ha mantenido, se interpreta como resultado con valor lógico "0", mientras que, si ha cambiado, se interpreta como valor lógico "1".

Con el método de la invención es posible generar números verdaderamente aleatorios a partir de celdas SRAM, independientemente de que las celdas consideradas tengan un mayor o menor sesgo hacia uno de los valores lógicos, por lo que cualquier celda SRAM puede ser explotada para TRNG.

Por tanto, y a diferencia de otros métodos, no es necesario ni disponer de un gran número de celdas SRAM del cuál seleccionar el pequeño subconjunto apropiado que pueda proporcionar números aleatorios con una calidad aceptable, ni someter los datos generados a un postprocesado intensivo que mejore la calidad, en términos de verdadera aleatoriedad, de los números aleatorios.

Además, en nodos tecnológicos futuros, incluso si las celdas SRAM tienden a ser aún más asimétricas debido a un mayor impacto de la variabilidad del proceso, este enfoque basado en DRV aún podría generar TRN a partir de cualquier celda.

5 Así, el método de la invención proporciona las siguientes ventajas:

- 1) No es necesario hacer una selección de celdas, sino que cualquier celda, sea simétrica o asimétrica, se puede utilizar como generador de números aleatorios, aprovechando todas las celdas disponibles.
- 2) Se consigue un mayor aumento de la entropía mínima que con otras técnicas, necesitando un postprocesado posterior mucho menor.
- 3) Se puede realizar el proceso de lectura a la tensión nominal de alimentación, a diferencia de otras técnicas, eliminando las dificultades técnicas de la lectura a una tensión muy reducida.

10

15

La generación de números aleatorios mediante el método de la invención puede ser aplicable en múltiples campos como en juego, en sistemas de telecomunicación o en muestreo estadístico, por ejemplo, para simulación. Pero la aplicación más destacada y en la cual la calidad, en cuanto a aleatoriedad, de los números generados tiene un mayor impacto es la criptografía, en tareas tales como la generación de claves, la generación de "nonces", o la generación de contramedidas frente a ataques.

20

Por otro lado, la invención también se refiere a un dispositivo para la generación de números verdaderamente aleatorios que comprende:

- Una o más celdas SRAM.
- Al menos una fuente de alimentación conectada a las celdas SRAM.
- Al menos un elemento de procesamiento conectado a la fuente de alimentación y a las celdas SRAM y configurado para controlar la tensión de la fuente de alimentación, para leer y escribir en las celdas SRAM y para llevar a cabo las etapas del método definido anteriormente.

25

30

El dispositivo para la generación de números verdaderamente aleatorios puede ser un chip que contiene una matriz de celdas SRAM. Preferentemente, las celdas SRAM son de 6 transistores.

35

La invención también se refiere a un programa de ordenador para la generación de números verdaderamente aleatorios configurado para llevar a cabo las etapas del

método de la invención definido en un elemento de procesamiento del dispositivo para la generación de números verdaderamente aleatorios de la invención.

5 Finalmente, la invención también se refiere a una unidad de almacenamiento configurada para almacenar el programa de ordenador definido.

10 El método y dispositivo objeto de esta invención son capaces de extraer aleatoriedad a partir de cualquier celda SRAM, es decir, el 100% de las celdas son útiles a efectos de generación de entropía; los procesos de lectura de las celdas son estándar y no necesita ningún equipamiento de alto coste.

DESCRIPCIÓN DE LOS DIBUJOS

15 Para complementar la descripción que se está realizando y con objeto de ayudar a una mejor comprensión de las características de la invención, de acuerdo con un ejemplo preferente de realización práctica de la misma, se acompaña como parte integrante de dicha descripción, un juego de dibujos en donde con carácter ilustrativo y no limitativo, se ha representado lo siguiente:

20 Figura 1.- Muestra la topología de una celda SRAM de 6 transistores (6T-SRAM) (estado de la técnica).

25 Figura 2.- Muestra una representación esquemática de los posibles escenarios en una celda SRAM cuando se escribe en ella su valor no preferido y se baja la tensión de alimentación desde su valor nominal a cualquier otro valor en el rango: 0 Voltios (V) a la tensión de alimentación (VDD) nominal.

30 Figura 3.- Muestra el método de determinación del DRV correspondiente al "1" lógico (DRV1).

Figura 4.- Muestra el método de determinación del DRV correspondiente al "0" lógico (DRV0).

35 Figura 5.- Muestra el método de determinación del DRV y valor lógico preferido de la celda SRAM a partir de DRV0 y DRV1.

Figura 6.- Muestra el método de generación de números aleatorios en una celda SRAM

REALIZACIÓN PREFERENTE DE LA INVENCION

5 La presente invención se refiere a un método para la generación de números verdaderamente aleatorios mediante el uso de celdas SRAM.

En las celdas SRAM, si una celda dada tiene un valor de DRV, y su valor no preferido está escrito en ella, pueden darse dos situaciones distintas, como se muestra en la Fig.

10 2:

- Si la tensión de alimentación de la celda se reduce a un valor considerablemente superior al DRV de la celda (201), la celda retendrá su valor almacenado.
 - Si la tensión de alimentación de la celda se reduce a un valor suficientemente por debajo del DRV de la celda (202), la celda sufrirá un cambio de bit hacia su
- 15 valor preferido.

Sin embargo, entre esas dos situaciones, hay un área intermedia, representada en la Fig. 2. Si la tensión de alimentación de la celda se reduce a un valor muy cercano al DRV de la celda, existe una probabilidad finita de que la celda cambie su valor almacenado, y, por tanto, una probabilidad también finita de que la celda conserve su

20 valor almacenado.

Para aumentar la aleatoriedad, el DRV de cada celda debe determinarse con la mayor precisión posible, de modo que la tensión de alimentación pueda reducirse a un valor dentro de dicha área intermedia.

25

Así, para generar bits aleatorios se sigue un proceso en dos pasos:

1) Determinación del DRV.

30

El método de determinación del DRV sigue los pasos descritos en las Figs. 3 a 5. Para una tecnología dada, se espera que el valor de DRV de las celdas SRAM se encuentre comprendido dentro de un cierto rango, que denotaremos $[VDD_RMIN, VDD_RMAX]$, donde VDD_RMIN es el valor más bajo y VDD_RMAX es el más alto. Se determina el valor del DRV de cada celda escribiendo (303) en primer lugar un "1" lógico, utilizando un proceso de escritura convencional con la tensión de alimentación VDD fijada (302)

35

al valor nominal. A continuación, se baja (304) el valor de la tensión de alimentación VDD a un valor de la tensión de configuración, inicialmente establecido (301) al valor superior de dicho rango VDD_RMAX, subiendo (305) posteriormente el valor de tensión de alimentación VDD al valor nominal y haciendo un proceso de lectura (306) convencional de la celda para comprobar (307) si ha cambiado el valor lógico almacenado.

Si el valor lógico almacenado no varía, el proceso se repite iterativamente (309) disminuyendo (308) el valor de la tensión de configuración un cierto valor ΔV en cada iteración. Este proceso se repite hasta que, o bien se produce (310) un cambio del valor lógico almacenado para un cierto valor de la tensión de alimentación DRV1, o bien se alcanza (311) el valor inferior del rango en el que se puede encontrar el DRV, fijando dicho valor como DRV1.

Así, el valor de ΔV determina la precisión con la que se determina DRV1.

A continuación, se repite el mismo proceso escribiendo un "0" lógico para determinar la tensión de alimentación DRV0 en que se produce un cambio del valor lógico almacenado.

Como se ha explicado, se determina el valor del DRV0 de cada celda escribiendo (403) en primer lugar un "0" lógico, utilizando un proceso de escritura convencional con la tensión de alimentación VDD fijada (402) al valor nominal. A continuación, se baja (404) el valor de la tensión de alimentación VDD a un valor de la tensión de configuración, inicialmente establecido (401) al valor superior de dicho rango VDD_RMAX, subiendo (405) posteriormente el valor de tensión de alimentación VDD al valor nominal y haciendo un proceso de lectura (406) convencional de la celda para comprobar (407) si ha cambiado el valor lógico almacenado.

Si el valor lógico almacenado no varía, el proceso se repite iterativamente (409) disminuyendo (408) el valor de la tensión de configuración un cierto valor ΔV en cada iteración. Este proceso se repite hasta que, o bien se produce (410) un cambio del valor lógico almacenado para un cierto valor de la tensión de alimentación DRV0, o bien se alcanza el valor inferior del rango en el que se puede encontrar el DRV, fijando (411) dicho valor como DRV0.

Una vez determinados DRV0 (502) y DRV1 (501), el mayor valor (503) entre DRV0 y DRV1 se almacena como valor de DRV de la celda y el correspondiente valor lógico constituye el valor no preferido de la celda, siendo (504) $DRV=DRV1$ si DRV1 es mayor que DRV0 y (505) $DRV=DRV0$ si DRV1 es menor que DRV0.

5

Este primer paso no es necesario ejecutarlo cada vez que se desean generar números verdaderamente aleatorios. Solo hay que hacerlo la primera vez y cuando se desee reajustar el valor almacenado de DRV, que puede haber cambiado por envejecimiento, temperatura, etc.

10

Este proceso puede realizarse periódicamente de una manera preestablecida, o bien, mediante un control de la calidad de los números aleatorios generados, por ejemplo, mediante el cálculo de la entropía mínima de los TRN.

15

2) Generación de entropía.

Una vez conocido el valor de DRV de cada celda y su valor no preferido, el método de generación de números aleatorios procede a través de los siguientes pasos, ilustrados gráficamente en la Fig. 6:

20

(1) Se almacena (602) en la celda su valor no preferido usando un procedimiento de escritura convencional fijando (601) la tensión nominal como tensión de alimentación de la celda.

25

(2) Se baja (603) la tensión de alimentación de la celda al valor determinado de su DRV (la celda puede entonces tanto cambiar como mantener el valor almacenado).

30

(3) Se sube (604) la tensión de alimentación de la celda a su valor nominal.

(4) Se lee (605) el contenido de la celda con un proceso de lectura convencional con tensión de alimentación VDD igual a la tensión nominal y se compara (606) con el valor previamente escrito.

(5) Se genera un bit verdaderamente aleatorio tomando el mantenimiento (608) del valor lógico almacenado como un cierto valor lógico, en este caso "0" lógico, y el cambio (607) del valor almacenado como el contrario, "1" lógico.

El método de la invención se puede utilizar para una única celda SRAM, aplicando el método repetidamente se pueden obtener tantos bits verdaderamente aleatorios como se desee.

5 Alternativamente, se puede utilizar el método de la invención con un conjunto de celdas SRAM, clasificando las celdas en subconjuntos de igual valor de DRV, determinados por la granularidad ΔV usada. La aplicación del método de generación de números verdaderamente aleatorios a todas las celdas de un subconjunto permite obtener tantos bits como celdas en cada aplicación del procedimiento.

10

Alternativamente, el método de generación de números verdaderamente aleatorios se puede aplicar para los distintos valores de DRV de los subconjuntos. En este caso, la totalidad de las celdas de la SRAM se puede utilizar para la generación de números aleatorios.

15

Se ha de notar que en el método de la invención las etapas para generar números verdaderamente aleatorios y para obtener una tensión de retención de datos de una celda y un valor lógico preferido son muy similares por lo que hay una correlación directa entre las mismas.

20

Como ilustración de la aplicabilidad del objeto de la invención, a continuación, se presentan los resultados obtenidos con un chip que contiene una matriz de 832 celdas SRAM fabricado en una tecnología CMOS de 65nm de longitud de canal. Las celdas SRAM 6T se han dimensionado con $W=80\text{nm}$ y $L=60\text{nm}$ para los transistores de acceso y los transistores PMOS de los inversores acoplados, y $W=160\text{nm}$ y $L=60\text{nm}$ para los transistores NMOS de los inversores acoplados, siguiendo los criterios de dimensionamiento convencionales de esta topología de celdas SRAM.

25

La aleatoriedad de los bits generados se ha cuantificado utilizando una métrica muy extendida: la entropía promedio mínima (H_{min}), definida como:

30

$$H_{min} = -\frac{1}{n} \sum_{i=1}^n \log_2(p_{imax})$$

donde p_{imax} es el máximo entre p_0 y p_1 para cada una de las n celdas. La aleatoriedad de los números aleatorios es mejor cuanto mayor sea la entropía mínima.

35

Se han realizado un conjunto de pruebas basadas en DRV, de acuerdo con el método de la invención, en las que se ha variado el tamaño de paso con el que se determina la DRV.

- 5 Los resultados de H_{min} para las diferentes pruebas basadas en DRV se muestran en la Tabla 1.

ΔV en el método basado en DRV (mV)	H_{min}
50	$2.32 \cdot 10^{-2}$
20	$3.12 \cdot 10^{-2}$
10	$5.45 \cdot 10^{-2}$
5	$8.60 \cdot 10^{-2}$
2	$1.68 \cdot 10^{-1}$
1	$2.09 \cdot 10^{-1}$

Tabla 1.

- 10 En las pruebas realizadas con el método de la invención, basadas en DRV, se ha variado el tamaño del paso (ΔV) y, por lo tanto, la precisión con la que se determinó el DRV. Como se ha explicado previamente, el procedimiento se puede dividir en dos partes:

- Determinación de DRV: se determina el DRV de cada celda escribiendo su valor no preferido y luego reduciendo su tensión de alimentación con un tamaño de paso dado ΔV y aumentándolo nuevamente después de cada paso a su tensión de alimentación nominal para leer el valor almacenado y verificar si el valor no preferido ha cambiado (bit-flip). El valor de la tensión de alimentación en el que la celda sufrió ese cambio (bit-flip) se registra como el DRV de la celda.
- Generación de entropía: una vez determinado el DRV de una celda, se genera entropía grabando su valor no preferido, bajando la tensión de alimentación a su DRV, volviendo a subir la tensión de alimentación a su valor nominal y leyendo el valor. Este proceso se ha repetido 200 veces para cada celda.

25

La entropía mínima obtenida en la Tabla I supera hasta en dos órdenes de magnitud la que se puede conseguir con un proceso convencional de encendido sobre el mismo tipo de celda en la misma tecnología. Cuando las pruebas mostradas en la Tabla I se

comparan entre sí, se puede ver cómo aumenta la entropía cuando se reduce el tamaño de paso utilizado para la determinación de DRV. Esto concuerda con lo esperado, ya que una mejor determinación del DRV, y por ende del área intermedia en la Fig. 2, incrementará las posibilidades de habilitar ambos posibles resultados. Por lo tanto, en una implementación práctica, se debe considerar un compromiso entre la capacidad de generar entropía y la factibilidad técnica de implementar un tamaño de paso más pequeño.

Esto demuestra que el método basado en DRV puede generar entropía incluso a partir de celdas que se etiquetarían como completamente estables para el método basado en encendido (que son la gran mayoría de las celdas). Esto se traduce en la posibilidad de utilizar un conjunto de celdas mucho más pequeño para garantizar la generación de números verdaderamente aleatorios.

15

REIVINDICACIONES

1. Método para la generación de números verdaderamente aleatorios mediante el uso de celdas SRAM que comprende las etapas de:
- 5 - obtener una tensión de retención de datos (DRV) de una celda y un valor lógico preferido;
 - colocar (601) la celda en un valor de tensión de alimentación nominal (VDD);
 - escribir (602) el valor lógico no preferido en la celda;
 - reducir (603) la tensión de alimentación de la celda a un valor de tensión
10 próximo a la tensión de retención de datos (DRV);
 - aumentar (604) la tensión de alimentación de la celda hasta el valor de tensión de alimentación nominal (VDD);
 - realizar un proceso de lectura (605) para comprobar (606) si se ha mantenido el valor lógico no preferido:
 - 15 o si se ha mantenido (608), se interpreta el valor extraído para el número verdaderamente aleatorio (del inglés, True Random Number TRN) como un valor lógico; y
 - o si ha cambiado (607), se interpreta como el valor lógico contrario.
- 20 2. Método de acuerdo con la reivindicación 1, donde la etapa de obtener la tensión de retención de datos de una celda y el valor lógico preferido comprende los pasos de:
- a) determinar un rango de posibles valores de tensión de retención de datos;
 - b) escribir (303) un valor "1" lógico;
 - 25 c) reducir (304) el valor de la tensión de alimentación (VDD) desde el valor nominal, previamente fijado (302), al valor más alto del rango determinado;
 - d) aumentar (305) el valor de tensión de alimentación al valor nominal;
 - e) realizar un proceso de lectura (306) para comprobar (307) si ha cambiado el valor lógico almacenado;
 - 30 f) repetir (309) los pasos c) a e) disminuyendo (308) el valor de tensión una cantidad ΔV iterativamente hasta:
 - o detectar (310) un cambio del valor lógico almacenado para un cierto valor de la tensión de alimentación, fijando dicho valor como DRV1;
 - o
 - 35 o alcanzar (311) el valor inferior del rango determinado, fijando dicho valor inferior como DRV1;

- g) repetir los pasos b) a f) escribiendo (403) un "0" lógico para determinar la tensión de alimentación DRV0;
- h) determinar DRV como el mayor valor (503) entre DRV0 y DRV1 y fijar el valor lógico correspondiente al mayor valor entre DRV0 y DRV1 como el valor no preferido de la celda.

5

3. Método de acuerdo con cualquiera de las reivindicaciones 1 a 2, donde se aplica el método a un conjunto de celdas SRAM.

10

4. Método de acuerdo con la reivindicación 3, que además comprende una etapa de clasificar las celdas en subconjuntos de igual valor de DRV.

5. Método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además una etapa de cuantificación de la aleatoriedad de los bits generados mediante la entropía mínima (H_{min}) calculada como:

15

$$H_{min} = -\frac{1}{n} \sum_{i=1}^n \log_2(p_{imax})$$

donde p_{imax} es el máximo entre la probabilidad de que cada celda vaya hacia el valor lógico "0" (p_0) y la probabilidad de que la celda vaya hacia el valor lógico "1" (p_1) durante un proceso de encendido, "n" es el número de celdas considerado e "i" es un valor comprendido entre 1 y "n".

20

6. Dispositivo para la generación de números verdaderamente aleatorios que comprende:

- una o más celdas SRAM;
- al menos una fuente de alimentación conectada a las celdas SRAM;
- al menos un elemento de procesamiento conectado a la fuente de alimentación y a las celdas SRAM y configurado para controlar la tensión de la fuente de alimentación, para leer y escribir en las celdas SRAM y para llevar a cabo las etapas de las reivindicaciones 1 a 6.

25

30

7. Dispositivo para la generación de números verdaderamente aleatorios de acuerdo con la reivindicación 6, donde el dispositivo es un chip que contiene una matriz de celdas SRAM.

8. Dispositivo para la generación de números verdaderamente aleatorios de acuerdo con la reivindicación 7, donde las celdas SRAM son de 6 transistores.
- 5 9. Programa de ordenador para la generación de números verdaderamente aleatorios configurado para llevar a cabo las etapas de acuerdo con las reivindicaciones 1 a 5 en un elemento de procesamiento de un dispositivo para la generación de números verdaderamente aleatorios de acuerdo con las reivindicaciones 6 a 8.
- 10 10. Unidad de almacenamiento configurada para almacenar el programa de ordenador de acuerdo con la reivindicación 9.

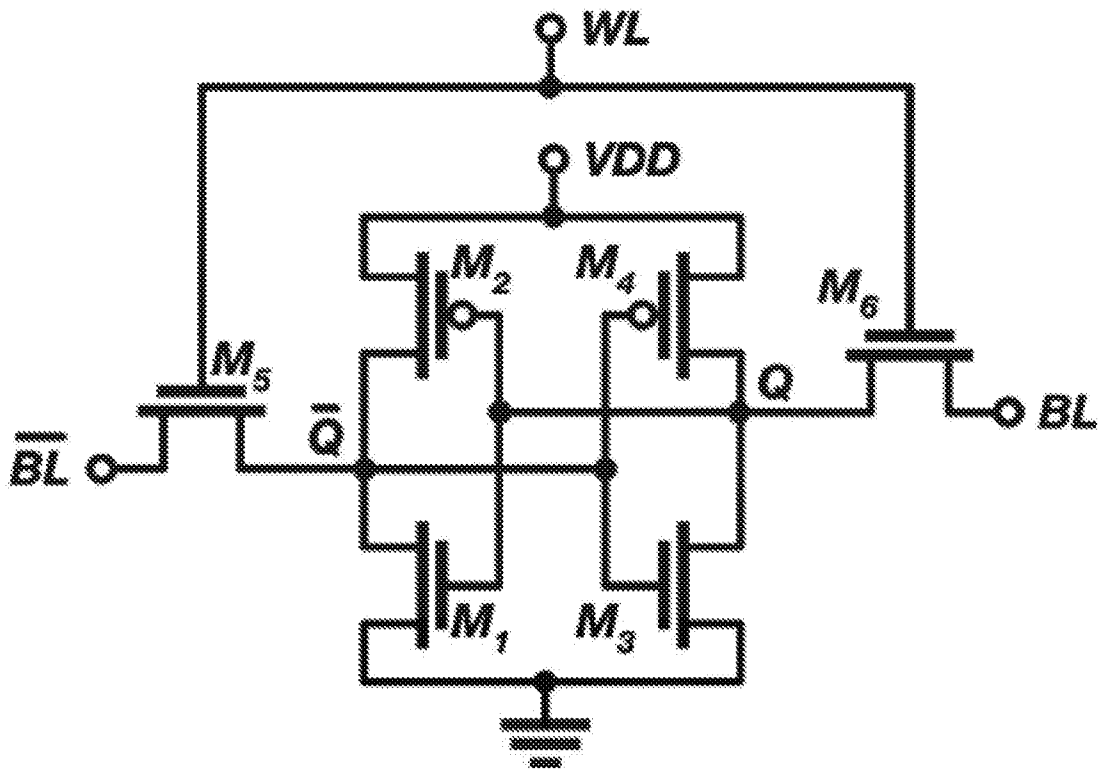


FIG. 1

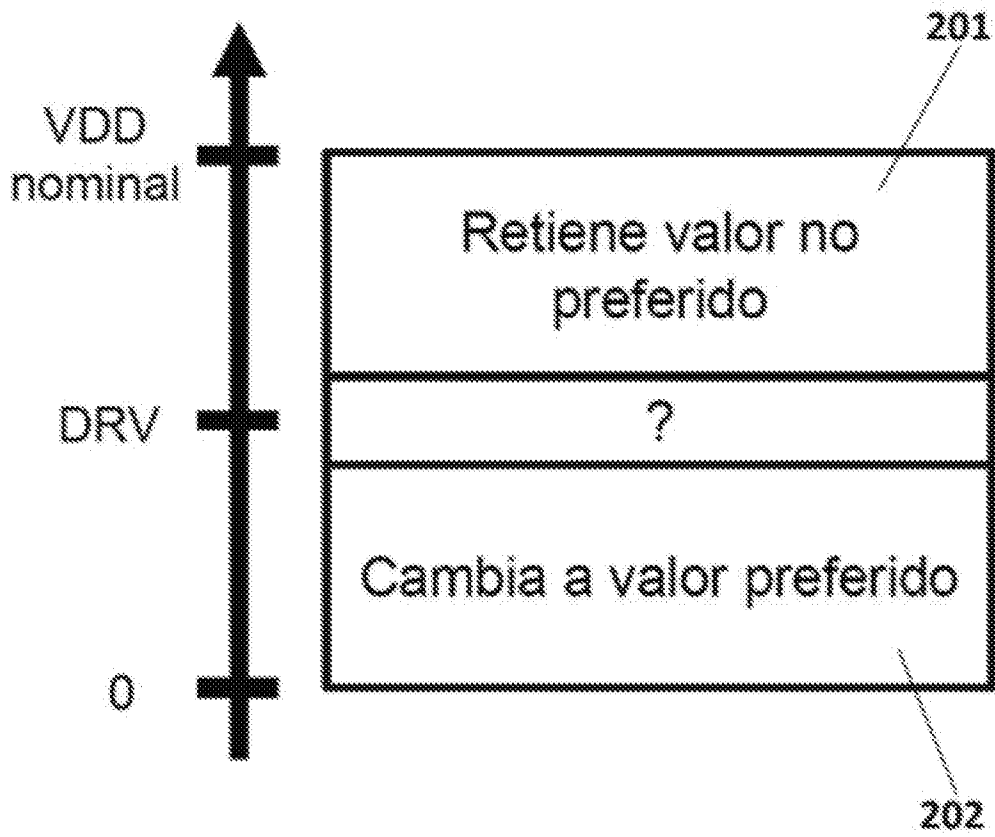


FIG. 2

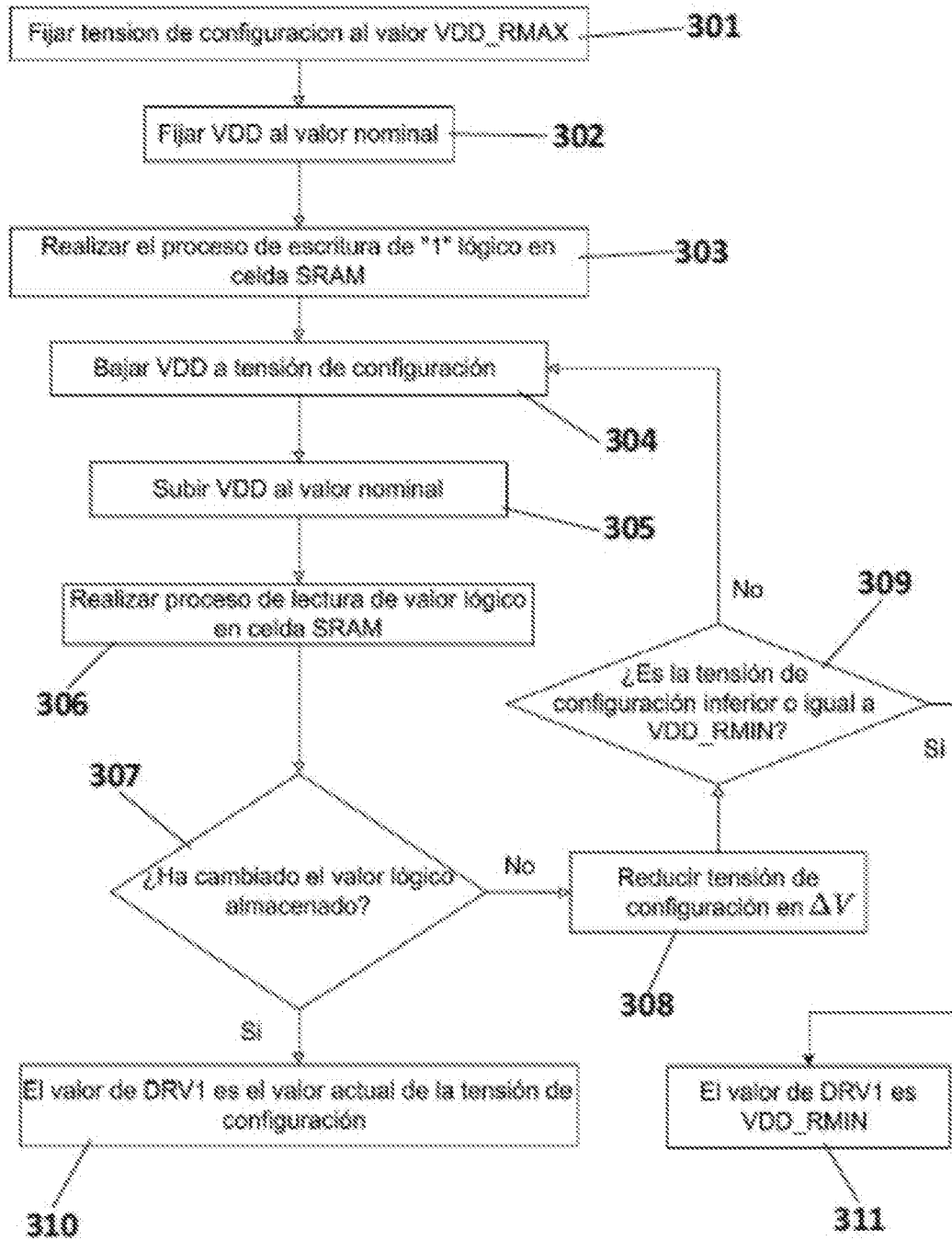


FIG. 3

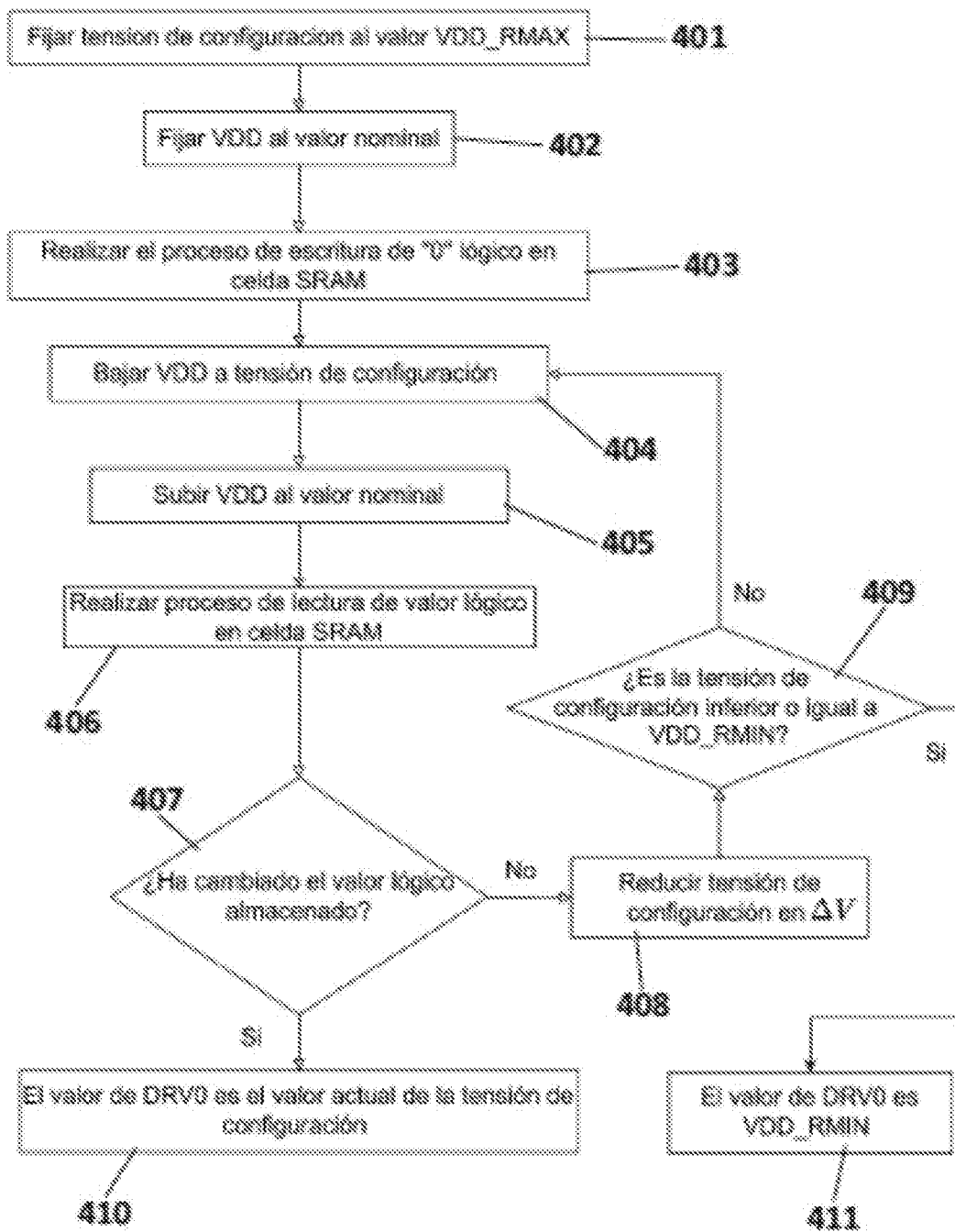


FIG. 4

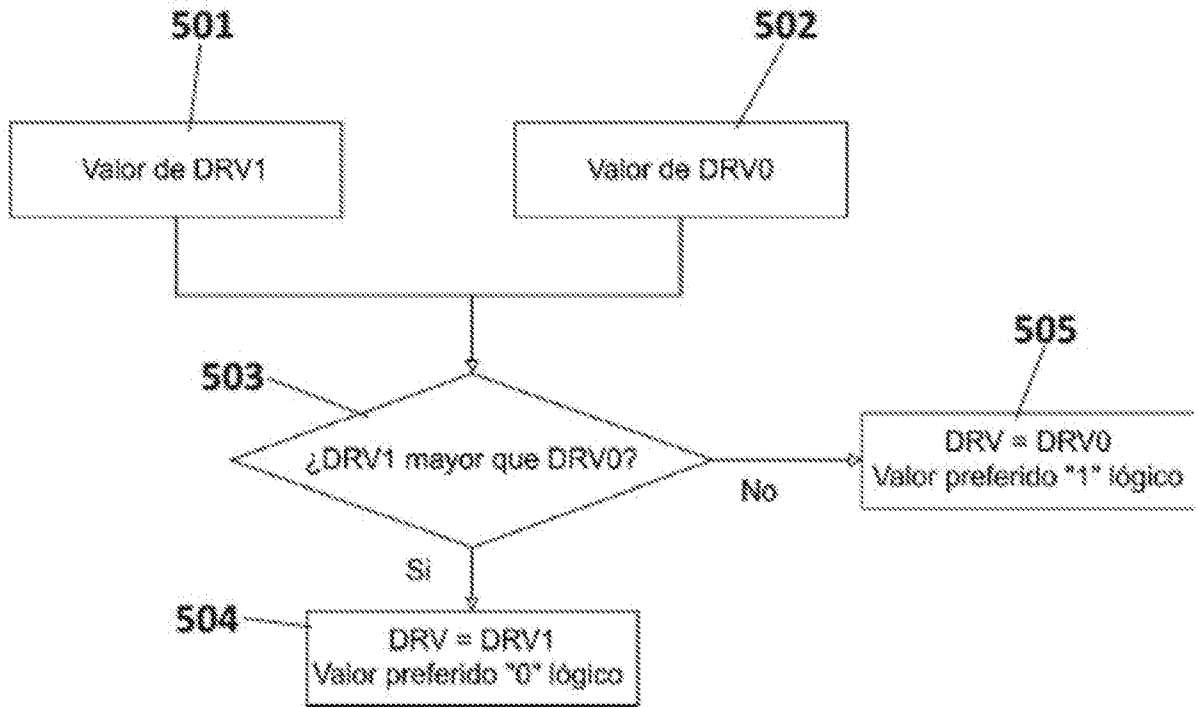


FIG. 5

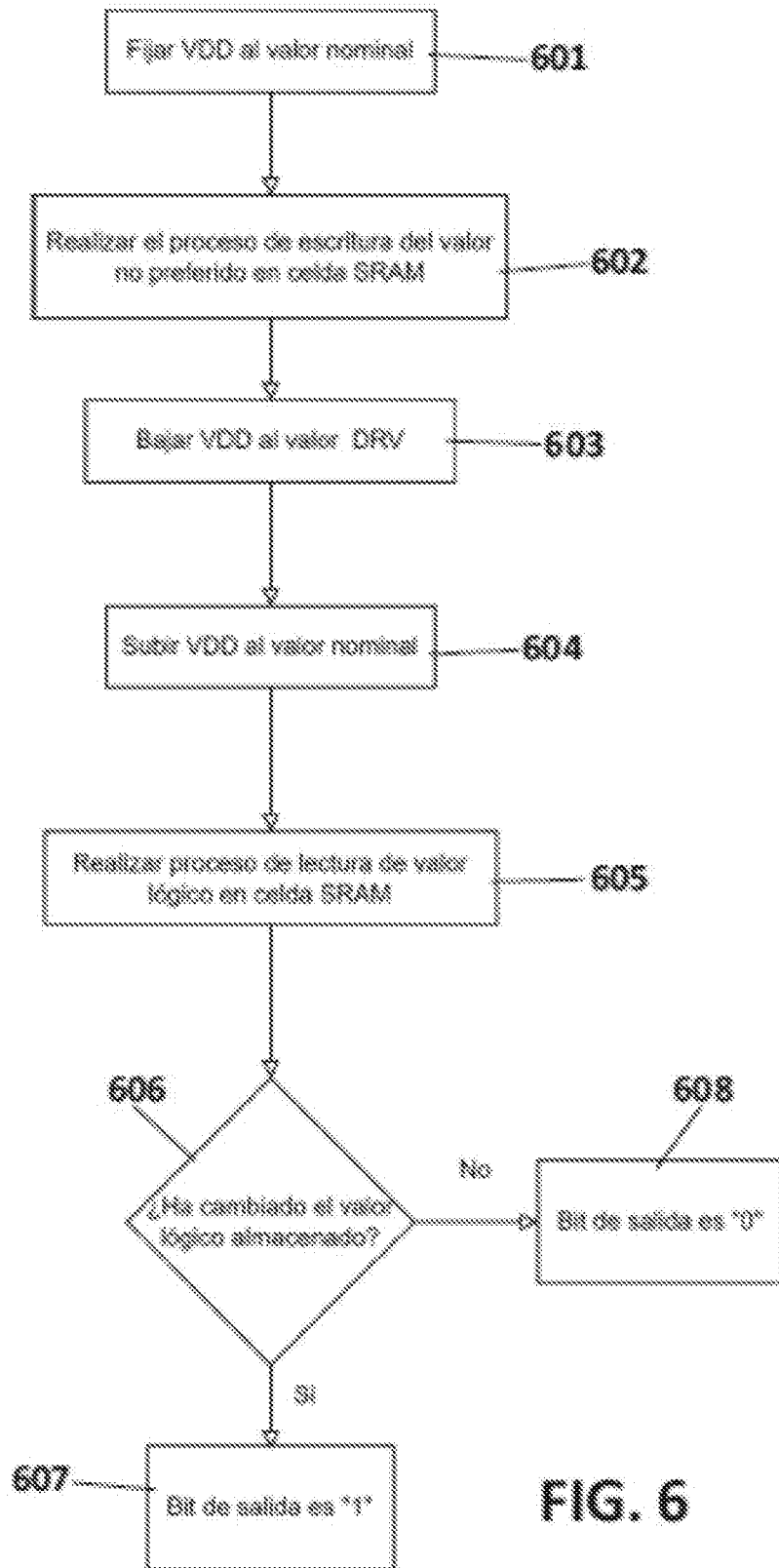


FIG. 6



- ②1 N.º solicitud: 202230569
②2 Fecha de presentación de la solicitud: 24.06.2022
③2 Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

⑤ Int. Cl.: **G06F7/58** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	⑤6 Documentos citados	Reivindicaciones afectadas
A	ES 2548792 A1 (UNIV SEVILLA et al.) 20/10/2015, resumen WPI, resumen EPODOC; páginas 2-25; reivindicaciones 1, 5, 11; figuras 2, 6, 7.	1-10
A	ELENA I. VATAJELU et al.: "Statistical analysis of 6T SRAM data retention voltage under process variation". Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2011 IEEE 14th International Symposium on, 20110413 IEEE, 13/04/2011, Páginas 365 - 370 [en línea][recuperado el 15/12/2022], ISSN ISBN 978-1-4244-9755-3 ; ISBN 1-4244-9755-8, <DOI: doi:10.1109/DDECS.2011.5783112>. Todo el documento.	1-10
A	LEOCHICO KESTER et al.: "Data retention voltage analysis of various low-power SRAM topologies". 2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS), 20140803 IEEE, 03/08/2014, Páginas 913 - 916 [en línea][recuperado el 15/12/2022], ISSN 1548-3746 ISBN 978-1-4799-4134-6 ; ISBN 1-4799-4134-4, <DOI: doi:10.1109/MWSCAS.2014.6908564>. Todo el documento.	1-10
A	NOA EDRI et al.: "Data retention voltage detection for minimizing the standby power of SRAM arrays". Electrical & Electronics Engineers in Israel (IEEEI), 2012 IEEE 27th Convention of, 20121114 IEEE, 14/11/2012, Páginas 1 - 5 [en línea][recuperado el 15/12/2022], ISSN ISBN 978-1-4673-4682-5; ISBN 1-4673-4682-9, <DOI: doi:10.1109/IEEEI.2012.6377025>. Todo el documento.	1-10
A	FARAH B. YAHYA et al.: "A novel technique to measure data retention voltage of large SRAM arrays". Circuits and Systems (ISCAS), 2011 IEEE International Symposium on, 20110515 IEEE, 15/05/2011, Páginas 65 - 68 [en línea][recuperado el 15/12/2022], ISSN ISBN 978-1-4244-9473-6; ISBN 1-4244-9473-7, <DOI: doi:10.1109/ISCAS.2011.5937502>. Todo el documento.	1-10

Categoría de los documentos citados

- X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica

- O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

- para todas las reivindicaciones para las reivindicaciones nº:

Fecha de realización del informe
15.12.2022

Examinador
M. T. Ibáñez Blanco

Página
1/2

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

G06F

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

INVENES, EPODOC