(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 548 792**

(21) Número de solicitud: 201400225

(51) Int. Cl.:

G06F 7/58 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

20.03.2014

(43) Fecha de publicación de la solicitud:

20.10.2015

Fecha de la concesión:

20.07.2016

(45) Fecha de publicación de la concesión:

28.07.2016

(56) Se remite a la solicitud internacional:

PCT/ES2015/000038

(73) Titular/es:

UNIVERSIDAD DE SEVILLA (85.0%)
Paseo de las Delicias s/n - Pabellón de Brasil
41013 Sevilla (Sevilla) ES y
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTIFICAS (15.0%)

(72) Inventor/es:

BATURONE CASTILLO, María Iluminada;
EIROA LORENZO, Susana y
PRADA DELGADO, Miguel Angel

(74) Agente/Representante:

GONZÁLEZ CARVAJAL, Ramón

(54) Título: **Método y dispositivo para generar identificadores y números verdaderamente aleatorios**

(57) Resumen:

La presente invención tiene por objeto un método que consta de dos etapas: una primera etapa de clasificación de las celdas de memoria estáticas en dos conjuntos disjuntos según su comportamiento ante repetidas veces en que se conectan a alimentación tras haber estado un tiempo suficiente sin alimentación, de manera que las celdas de uno de los conjuntos son adecuadas para generar identificadores (claves o secretos) y las del otro son adecuadas para generar números verdaderamente aleatorios. Gracias a esta clasificación, en la segunda etapa de generación de números, los identificadores así como los números aleatorios generados ofrecen mejores prestaciones. También es objeto de la invención el dispositivo para implementar el método propuesto que puede realizarse añadiendo circuitería muy simple a la memoria o ejecutando un software muy sencillo. Las áreas científico-técnicas a las que se puede corresponder el invento son las de Criptografía, Tecnología Electrónica, Seguridad y Privacidad.

ES 2 548 792 B1

DESCRIPCIÓN

Método y dispositivo para generar identificadores y números verdaderamente aleatorios

Objeto de la invención

La presente invención tiene por objeto un método que consta de dos etapas: una primera etapa de clasificación de las celdas de memoria estáticas en dos conjuntos disjuntos según su comportamiento ante repetidas veces en que se conectan a alimentación tras haber estado un tiempo suficiente sin alimentación, de manera que las celdas de uno de los conjuntos son adecuadas para generar identificadores (claves o secretos) y las del otro son adecuadas para generar números verdaderamente aleatorios. Gracias a esta clasificación, en la segunda etapa de generación de números, los identificadores así como los números aleatorios generados ofrecen mejores prestaciones. También es objeto de la invención el dispositivo para implementar el método propuesto que puede realizarse añadiendo circuitería muy simple a la memoria o ejecutando un software muy sencillo. Las áreas científico-técnicas a las que se puede corresponder el invento son las de Criptografía, Tecnología Electrónica, Seguridad y Privacidad.

Estado de la técnica

Las celdas de memoria estáticas se caracterizan porque poseen dos estados estables, de forma que mantienen el dato binario (valor lógico "0" ó "1") que se les escribe mientras están alimentadas, pero pierden la información si se les interrumpe la alimentación. Si se alimentan pero no se les escribe ningún dato, las celdas evolucionan hacia un valor u otro de una forma que es difícil de predecir, modelar matemáticamente y clonar físicamente, por lo que es muy difícil obtener un conjunto de celdas que se comporten de la misma forma. Aprovechando estas características, estas celdas se han empleado para generar identificadores de circuitos y números verdaderamente aleatorios.

Las celdas de memoria estáticas están constituidas por circuitos acoplados en cruz, como latches, flip-flops, puertas NOR, inversores, etc. En [Kumar2008] se proponen celdas basadas en dos latches en cruz para identificar FPGAs. En [Maes2008] se

propone el uso de flip-flops para identificar FPGAs. En [Su2008] se proponen celdas basadas en dos puertas NOR en cruz para identificar circuitos integrados de aplicaciones específicas. En [Layman2004] se propone un método que emplea celdas basadas en dos inversores en cruz (las típicas que forman las memorias estáticas de acceso aleatorio, SRAMs) para identificar las obleas de circuitos integrados y/o los dados en que se divide cada oblea.

En aplicaciones de identificación, se suele usar una técnica reto-respuesta con las celdas de memoria para identificar el dispositivo en el que esté incluida la memoria, de modo que el reto sean las celdas que se van a emplear y las respuestas sean los valores a los que se estabilizan las celdas cuando se les conecta la alimentación [Guajardo2007] [Holcomb2009] [Kim2010] [Gebara2012]. También se han propuesto otros métodos que combinan las respuestas de las celdas. En estas aplicaciones siempre es necesaria una etapa de registro en la que a cada dispositivo se le asigna un identificador, ID. En la etapa de identificación, se calcula la distancia (normalmente una distancia de Hamming, HD) entre el ID generado por el dispositivo y los registrados y se identifica el dispositivo como aquel cuyo ID registrado presente la menor distancia. En aplicaciones de autenticación solo se registra un dispositivo, de modo que en la etapa de autenticación se calcula la distancia entre el ID generado y el registrado y si la distancia está por debajo de un umbral, el dispositivo se considera auténtico, y si no, el dispositivo se considera falso. La calidad de una técnica de identificación/autenticación se suele evaluar midiendo las razones de falso rechazo (FRR, "False Rejection Rate") y de falsa aceptación (FAR, "False Acceptance Rate") para cada valor de umbral elegido. Lo ideal es que exista al menos un valor de umbral para el que no haya dispositivos auténticos rechazados como falsos (FRR=0) y, a la vez, no haya dispositivos falsos aceptados como auténticos (FAR=0). De forma equivalente, también se representan los porcentajes de población genuina (auténtica) e impostora frente a cada valor de umbral elegido. Lo ideal es que ambas poblaciones estén claramente separadas.

En aplicaciones de identificación/autenticación interesa que las celdas proporcionen siempre el mismo valor. Sin embargo, hay celdas que proporcionan un valor en la etapa de identificación distinto al que se les asignó en la etapa de registro. Hay celdas de memoria que presentan una tendencia clara a estabilizarse en un valor u otro y celdas que no presentan ninguna tendencia clara (su valor de inicialización es distinto cada vez que se las alimenta). En [Holcomb2009] las celdas de SRAMs se clasifican dependiendo de sus curvas de transferencia de tensión ("Voltage Transfer Curves" o

VTCs) en celdas asimétricas ("skewed cells"), que presentan una probabilidad mayor para estabilizarse en un valor que en otro, y celdas simétricas ("neutral cells"), que no presentan ninguna tendencia clara a un valor u otro. Uno de los motivos por los que una celda es de un tipo u otro son las variaciones que haya habido en el proceso de fabricación de la memoria, que dan lugar a que los dos circuitos en cruz constitutivos de cada celda no sean perfectamente idénticos. Las celdas que son asimétricas por este motivo son las más adecuadas a la hora de generar identificadores pues caracterizan la naturaleza intrínseca, única e irrepetible de la memoria. Pero las variaciones en el proceso de fabricación no son el único motivo. Las memorias presentan remanencia, es decir, valores previos almacenados en las celdas pueden influir en los valores futuros a los que evolucionen las celdas si el tiempo que está la memoria apagada es corto. Aunque esta influencia se puede eliminar si el tiempo de apagado es suficiente (por ejemplo unas pocas decenas de segundos). Por otro lado, en el caso de SRAMs, se ha estudiado que el envejecimiento y el efecto NBTI (Negative Bias Temperature Instability), consecuencia de un uso prolongado de la SRAM, también provocan que una celda sea asimétrica o simétrica [Guajardo2007] [Holcomb2009]. Mucho más influyente que el motivo anterior a la hora de modificar el comportamiento de las celdas son las condiciones de operación, sobre todo la temperatura. La temperatura influye en las tensiones umbrales y en la movilidad electrón-hueco de los transistores CMOS que forman cada celda de memoria, de manera que un cambio de temperatura puede convertir una celda asimétrica en simétrica y viceversa [Kim2010] [Gebara2012]. Las variaciones en la tensión de alimentación también influyen considerablemente porque modifican el margen de ruido estático (Static Noise Margin, SNM) de las celdas, haciendo que sean más o menos susceptibles al ruido [Holcomb2009].

Para reducir el problema de celdas que proporcionan un valor en la etapa de identificación distinto al que se les asignó en la etapa de registro se han propuesto distintas soluciones. La propuesta en [Holcomb2009] es promediar los valores a los que se estabilizan un conjunto dado de celdas de SRAMs para un número dado de medidas realizadas a la temperatura y tensión de alimentación nominales y, en base al promedio obtenido, asignar a cada celda el valor binario más probable para formar con ellos el identificador registrado. La propuesta en [Kim2010] es generar un identificador como en [Holcomb2009], pero no un solo identificador obtenido en condiciones de operación nominales, sino generar varios identificadores para varias condiciones de operación, fundamentalmente para varias temperaturas. Cuantos más IDs se registren

por cada SRAM, uno para cada temperatura, mejor será la caracterización de la SRAM. Como solución de compromiso entre buena caracterización y etapa de registro no demasiado costosa, se propone generar un ID para la máxima temperatura de operación, otro para la mínima y otro para el valor intermedio. La propuesta en [Gebara2012] extiende el trabajo en [Kim2010] y caracteriza las celdas de memoria alimentándolas con varios valores de tensión (desde 0.2Vdd a 1.4Vdd, con Vdd el valor nominal) durante un tiempo (aproximadamente 1 microsegundo) y luego ajustando la alimentación a su valor nominal antes de leer los valores a los que se estabilizan las celdas. Se realizan varias medidas a cada valor de tensión de alimentación y para cada valor de temperatura. La información que se almacena en la etapa de registro es, no solo el ID más probable por cada temperatura, sino también la probabilidad de cada celda de estabilizarse en un valor u otro. Incluso introducen la posibilidad de no usar las celdas de memoria cuyos valores cambien en distintas condiciones de temperatura. Para medir la distancia entre el ID generado en la etapa de identificación y el ID almacenado para cada temperatura en la etapa de registro, introducen una medida de similitud que pondera la distancia entre un bit generado y otro almacenado por la probabilidad registrada para esa celda y luego fusionan los resultados obtenidos con cada ID para cada temperatura. Para implementar esta técnica, se propone un sistema que pruebe a nivel de oblea las SRAMs incluidas en los circuitos integrados. El sistema para probar las obleas debe incluir una fuente de alimentación programable mediante un computador que fije la tensión de alimentación a los diferentes valores (de 0.2Vdd a 1.4Vdd durante aproximadamente 1 microsegundo) y luego la ajuste al valor nominal. Además, es necesaria una cámara de temperatura o un sistema de forzado de temperatura también programable por el computador. Esta propuesta está dirigida a fabricantes de semiconductores o vendedores especializados de circuitos integrados.

En aplicaciones de construcción dinámica de claves o secretos también interesa que las celdas proporcionen siempre el mismo valor. Para reducir el problema de celdas que no lo hacen, se suelen emplear algoritmos de datos públicos (Helper Data Algorithms o HDA), de entre los cuales, el más conocido es el HDA basado en offset de código (Code Offset-based HDA) que, como las aplicaciones de identificación/autenticación, posee una etapa de registro y otra de recuperación de secreto. En la fase de registro se llevan a cabo los siguientes pasos: (a) se obtiene una respuesta, R, a partir de varios valores de inicialización de celdas de memoria, (b) se elige una palabra de código aleatoria, C, de un código corrector de errores, (c) se

calcula un vector de datos públicos como W = XOR(C, R) y (d) se almacena W. En la fase de recuperación de secreto se llevan a cabo los siguientes pasos: (a) se obtiene una respuesta de la memoria de la misma forma que en la fase de registro, R' (como hay celdas que no siempre proporcionan el mismo valor, la respuesta R' no será idéntica a R, aunque sí similar), (b) se calcula C' = XOR(W, R') = XOR[XOR(C, R), R'], (c) se aplica a C' el algoritmo decodificador del código corrector de errores, de forma que si C' es próxima a C, el decodificador recupera C y, por lo tanto, se recupera R = XOR(W, C). El resultado de una función hash aplicada sobre R puede emplearse como clave criptográfica [Guajardo2007]. El paso más costoso de estos algoritmos es el de la decodificación del código corrector de errores. La complejidad de esta decodificación se reduce si el porcentaje de celdas que proporcionan siempre el mismo valor aumenta.

Los circuitos acoplados en cruz también se han empleado para diseñar generadores de números verdaderamente aleatorios (True Random Number Generators, TRNGs). La idea es usar los valores iniciales de las celdas como fuente de entropía, extrayendo el ruido que provoca que una celda en un estado meta-estable (que no es ninguno de sus dos estados estables) evolucione hacia uno de sus estados estables. La entropía es una medida matemática del desorden, aleatoriedad o variabilidad. De acuerdo a las recomendaciones del NIST (National Institute of Standards and Technology), la entropía mínima es la medida en el peor caso de la incertidumbre de una variable aleatoria, es decir, que proporciona el máximo valor que puede tomar la probabilidad de acertar el valor de la variable aleatoria. La mínima entropía de una fuente binaria, como puede serlo una celda de memoria, se define como:

$$H_{min} = -\log_2(p_{max})$$

donde p_{max} es la máxima de las probabilidades que presenta una celda de tomar un "0" o un "1".

Suponiendo que todos los bits que proporcionan las celdas cuando se les conecta la alimentación son independientes, cada secuencia de n bits presenta la siguiente entropía mínima total:

$$(H_{min})_{total} = -\sum_{i=1}^{n} \log_2(pi_{max})$$

En las aplicaciones de generación de números verdaderamente aleatorios, al contrario que en las aplicaciones de generación de identificadores o construcción dinámica de secretos, interesa que las celdas proporcionen distinto valor cada vez que se alimenten para que la entropía mínima total aumente. Las celdas asimétricas no son adecuadas para generar aleatoriedad puesto que su comportamiento se puede predecir. Son mucho más adecuadas las celdas simétricas. Se ha propuesto incluir circuitería adicional que controle el nivel de ruido original de las celdas y las ajuste para que operen en régimen de meta-estabilidad. Otros autores han propuesto incluir también circuitería para evaluar la calidad de los números aleatorios conforme se van generando. Otra opción es procesar los bits para mejorar sus propiedades estadísticas. Una solución clásica es aplicar un operador XOR o un corrector de Von Neumann. En la solicitud de patente [Harris2011] se propone el procesado de los bits de inicialización generados mediante un circuito corrector de errores. Para conseguir una secuencia de n bits verdaderamente aleatoria, la propuesta en [Holcomb2009] es emplear una función de compresión (en concreto una función hash PH) que comprima a n bits una secuencia de muchos más bits, tantos más cuanto menor sea la entropía mínima total que se haya obtenido. El trabajo en [Leest2012] emplea como función hash una SHA-256. La patente en [Nishino2005] también propone el uso de funciones hash, preferentemente los algoritmos MD2, MD4 ó MD5. Los valores de entropía mínima total reportados para memorias SRAMs suelen ser bajos, porque la mayoría de las celdas se estabiliza siempre al mismo valor. Así por ejemplo, se reporta en [Holcomb2009] que para obtener un número de 128 bits que supere las pruebas estadísticas de aleatoriedad se necesitan 4096 bits y en [Leest2012] se reporta que para obtener un número de 256 bits se necesitan 12800 bits (en [Leest2012] se contemplan distintas temperaturas de operación para la memoria). Cuantos más bits sean necesarios (porque menor sea la entropía mínima total), más lenta es la generación de los números aleatorios.

Los números auténticamente aleatorios se usan en multitud de algoritmos de cifrado y protocolos seguros de comunicación. En muchos casos, se emplean como semilla para inicializar algoritmos de generación de números pseudo-aleatorios, como se propone en [Leest2012]. En [Handschuh2012], los números aleatorios también se derivan de los bits de inicialización de la memoria de una forma indirecta, usando un generador de números aleatorios determinista.

Bibliografía

[Gebara2012] *F. H. Gebara, J. Kim, J. D. Schaub, and V. Strumpenl. "Temperature-profiled device fingerprint generation and authentication from power-up states of static cells". US Patent 8,219,857 B2, July 2012.*

[Guajardo2007] *J. Guajardo, S. Kumar, G.J. Schrijen, and P. Tuyls. "FPGA intrinsic PUFs and their use for IP protection". Proc. of Cryptographic Hardware and Embedded Systems (CHES), pages 63–80, 2007.*

[Handschuh2012] *H. Handschuh, G.J. Schrijen, E. Van der Sluis, "Random number generating system based on memory start-up noise", PCT/EP2012/056277, Oct. 2012.*

[Harris2011] *E.B. Harris, R. Hogg, R.A. Kohler, R.J. McParland, and W.E. Werner, "Secure random number generator", US Patent Aplication US 2011/0022648 A1, January 2011.*

[Holcomb2009] *D.E. Holcomb, W.P. Burleson, and K. Fu. "Power-up SRAM state as an identifying fingerprint and source of true random numbers". IEEE Transactions on Computers, 58(9), pages 1198–1210, 2009.*

[Kim2010] *J. Kim, J. Lee, and J.A. Abraham. "Toward reliable SRAM-based device identification". In Proc. IEEE International Conference on Computer Design (ICCD), pages 313–320, 2010.*

[Kumar2008] *S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijenand, P. Tuyls, "The butterfly PUF protecting IP on every FPGA", in Proc. 1st IEEE Int. Workshop on Hardware-Oriented Security and Trust, HOST, 2008.*

[Layman2004] *P. A. Layman, S. Chaudhry, J. G. Norman, J. R. Thomson, "Electronic fingerprinting of semiconductor integrated circuits". US Patent 6,738,294, May 2004.*

[Leest2012] *V. van der Leest, E. van der Sluis, G.J. Schrijen, P. Tuyls, and H. Handschuh. "Efficient implementation of true random number generator based on SRAM PUFs". In Cryptography and Security: From Theory to Applications, pages 300–318. Springer, 2012.*

[Maes2008] *R. Maes, P. Tuyls, I. Verbauwhede. "Intrinsic PUFs from Flip-flops on reconfigurable devices". In: 3rd Benelux Workshop on Information and System Security (WISSec 2008), Eindhoven, NL, page 17, 2008.*

[Nishino2005] *Y. Nishino, "Methods and apparatus for random number generation". US Patent 7,676,531 B2, March 2010.*

[Su2008] *Y. Su, J. Holleman, and B. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," IEEE Journal of Solid-State Circuits, vol. 43, no. 1, pp. 69–77, Jan. 2008.*

Descripción de las figuras

Figura 1. Diagrama de flujo que ilustra los pasos de la primera fase del método de la invención.

Figura 2: Diagrama de flujo que ilustra los pasos de la segunda fase del método de la invención.

Figura 3: Porcentaje de celdas para las 20 muestras del circuito analizado que se estabilizan siempre al mismo valor en todas las condiciones de operación cuando: (a) se contemplan todas las celdas de la memoria porque no se ha aplicado el método de la invención (en trazo negro continuo), (b) se contemplan sólo las celdas etiquetadas como A al realizar una vez la primera fase del método de la invención contemplando tres valores de tensión de alimentación y la misma temperatura (en trazo gris continuo) y (c) se contemplan sólo las celdas etiquetadas como A al realizar tres veces la primera fase del método de la invención contemplando tres temperaturas de operación y la misma tensión de alimentación (en trazo discontinuo).

Figura 4: Poblaciones impostoras y genuinas para identificadores de 128 bits cuando los bits provienen de: (a) 128 celdas cualesquiera de la memoria porque no se ha aplicado el método de la invención (en trazo negro continuo), (b) 128 celdas etiquetadas como A al realizar una vez la primera fase del método de la invención contemplando tres valores de tensión de alimentación y la misma temperatura (en trazo gris continuo) y (c) 128 celdas etiquetadas como A al realizar tres veces la primera fase del método de la invención contemplando tres temperaturas de operación y la misma tensión de alimentación (en trazo discontinuo).

Figura 5: Entropía mínima total (en %) para las 4 muestras del circuito medida en (a) condiciones nominales, (b) el peor caso para condiciones en que varíe la tensión de alimentación y (c) el peor caso para condiciones en que varíe la temperatura de operación. En todas las figuras, se muestra en trazo negro continuo la entropía mínima total medida cuando se consideran las 2280 celdas de memoria (sin aplicar el método de la invención), en trazo gris continuo cuando se consideran las celdas etiquetadas como B al realizar una vez la primera fase del método de la invención contemplando tres valores de tensión de alimentación y la misma temperatura y en trazo discontinuo, cuando se consideran las celdas etiquetadas como B al realizar tres veces la primera fase del método de la invención contemplando tres temperaturas de operación y la misma tensión de alimentación.

Figura 6: Diagrama de bloques del dispositivo que implementa el método de la invención.

Figura 7: Esquemático que ilustra un ejemplo de realización del dispositivo empleando circuitería adicional en una FPGA para realizar los bloques de clasificación y control.

Descripción de la invención

El método propuesto en la presente invención tiene por objeto una nueva etapa de registro en la que las celdas de memoria se clasifican en dos conjuntos disjuntos, uno adecuado para generar identificadores (claves o secretos), y otro adecuado para generar números aleatorios. Gracias a esta clasificación, en la etapa de generación de números, los identificadores generados son más repetibles, con lo cual, pueden tener un número de bits menor para conseguir unas mismas prestaciones de identificación, se pueden generar claves o secretos reduciendo la complejidad de los códigos correctores de errores y se mejora la entropía de los números aleatorios generados. Además, todo ello se consigue con una misma etapa de registro, que puede repetirse para mejorar la calidad de los identificadores y números aleatorios generados en distintas condiciones de operación. El método puede aplicarse sin necesidad de un complejo y costoso montaje experimental (no son necesarias cámaras de temperatura o sistemas de forzado de temperatura), sino simplemente controlando la tensión de alimentación. Como consecuencia, la etapa de registro puede realizarse con la memoria en su contexto de aplicación, de una forma cómoda y sencilla. No es necesario que la etapa de registro se realice por vendedores especializados ni en la fábrica donde se fabrique la memoria. El dispositivo que se presenta en esta invención para implementar el método propuesto puede realizarse añadiendo circuitería muy simple a cualquier memoria estática o ejecutando un software muy sencillo. El dispositivo puede autenticarse sin necesidad de almacenar su identificador porque lo genera en tiempo de operación y, a la vez, puede comunicar de forma segura su identidad y cualquier otra información sensible haciendo uso de los números verdaderamente aleatorios que genera.

El método propuesto permite generar al menos un número de identificación de n bits y al menos un número verdaderamente aleatorio de m bits a partir de N celdas de memoria estáticas teniendo cada celda capacidad de almacenar un bit de información, en el cual n puede tomar valores desde 0 hasta N-m y m puede tomar valores desde 0 hasta N-n. El método se caracteriza porque comprende una primera fase en la que se

clasifican las N celdas de memoria en al menos dos grupos etiquetados como A y B, y una segunda fase en la que se generan al menos un número de identificación de n bits a partir de n celdas etiquetadas en la primera fase como A y al menos un número verdaderamente aleatorio de m bits a partir de m celdas etiquetadas en la primera fase como B, donde la primera fase de clasificación se lleva a cabo al menos una vez, de forma que, una vez clasificadas las celdas, la generación de números de identificación y aleatorios se puede llevar a cabo directamente ejecutando la segunda fase sin tener que volver a ejecutar la primera fase.

La primera fase del método a su vez comprende:

(a) dejar sin alimentación a la memoria (y, por tanto, a sus celdas) durante un tiempo suficiente para que desaparezcan todos los valores de los bits que pudieran estar almacenados,

(b) conectar la memoria a una tensión de alimentación fijada y leer los valores de los bits a los que se han estabilizado N celdas de memoria sin antes haber escrito nada en ellas,

(c) guardar los valores de los bits leídos de las N celdas,

(d) dejar sin alimentación a la memoria durante el tiempo suficiente para borrar los valores almacenados,

(e) alimentar de nuevo la memoria con el mismo valor de tensión y volver a leer los valores de bits de las N celdas sin antes haber escrito nada en ellas,

(f) comparar los valores de bits obtenidos en el paso (e) con los guardados en el paso (c), clasificando las celdas de memoria en dos grupos: las celdas que siempre proporcionan el mismo valor de bit y las celdas que alguna vez han proporcionado un valor de bit diferente,

(g) ir al paso (h) si ya se han tomado todas las medidas para el mismo valor de tensión de alimentación fijado; mientras que, en otro caso, volver al paso (d),

(h) etiquetar las celdas que siempre han proporcionado el mismo valor de bit para todas las medidas realizadas a un mismo valor de tensión como S, etiquetar las otras celdas como U y guardar el resultado de la clasificación para el valor de tensión analizada,

(i) ir al paso (j) si ya se han analizado todos los valores de tensión de alimentación; mientras que, en otro caso, fijar un nuevo valor de tensión de alimentación a analizar y volver al paso (a),

(j) comparar los resultados de clasificación obtenidos para los valores de tensión analizados y etiquetar las celdas de memoria que han sido etiquetadas siempre como S con todos los valores de tensión analizados con una etiqueta A y etiquetar las celdas que han sido etiquetadas siempre como U con todos los valores de tensión analizados con una etiqueta B (asignando una etiqueta C a las celdas que no se les asigna una etiqueta A ni B).

La Figura 1 muestra el diagrama de flujo que ilustra los pasos de la primera fase del método de la invención.

La segunda fase del método a su vez comprende:

(1) dejar sin alimentación a la memoria (y, por tanto, a sus celdas) durante un tiempo suficiente para que desaparezcan todos los valores de bits que pudieran estar almacenados,

(2) alimentar la memoria a su valor de tensión nominal, no escribir nada en las N celdas analizadas en la primera fase y generar una secuencia de bits (cadena-A) con los valores de bits a los que se hayan estabilizado las celdas etiquetadas como A y generar otra secuencia de bits (cadena-B) con los valores de bits de las celdas etiquetadas como B, finalizando la lectura cuando al menos se tenga una cadena-A de n bits y una cadena-B de m bits,

(3) utilizar la cadena-A para generar al menos un número de identificación digital de n bits y la cadena-B para generar al menos un número verdaderamente aleatorio de m bits.

La Figura 2 muestra el diagrama de flujo que ilustra los pasos de la segunda fase del método de la invención.

En la primera fase del método se analizan P valores de tensión de alimentación (siendo P mayor o igual a 1), de los cuales al menos uno es el valor de tensión nominal (Vdd). Si en la primera fase del método se analizan varios valores de tensión de alimentación, lo conveniente es analizar el intervalo de tensiones para el que la memoria puede trabajar con normalidad, que suele ser un 10% por encima y por debajo de Vdd. Por lo tanto, lo conveniente es analizar, además de Vdd, un valor

menor que el nominal Vdd_{min}=0.9Vdd y un valor mayor que el nominal Vdd_{max}=1.1Vdd. Como la memoria puede trabajar con normalidad, no es necesario desconectarla del resto de circuitería a la que pudiera estar conectada. Además, si la memoria forma parte de un dispositivo electrónico que también puede trabajar con esos niveles de tensión, a todo el dispositivo se le puede aplicar el método de la invención sin problema.

El método también se caracteriza porque al repetirse la primera fase del método, se etiquetan con una etiqueta A las celdas que en la anterior primera fase se etiquetaron con A y en la actual primera fase del método vuelven a etiquetarse como A; se etiquetan con una etiqueta B las celdas que en la anterior primera fase se etiquetaron con B y en la actual primera fase del método vuelven a etiquetarse como B y se etiquetan con una etiqueta C el resto de las celdas. Cuando se realiza la primera fase del método sin indicar que sea una repetición, se borra cualquier resultado de posibles clasificaciones anteriores y se almacena el resultado de la clasificación actual.

La repetición de la primera fase del método permite refinar la clasificación contemplando otras posibles condiciones de operación de la memoria.

Puesto que las SRAMs forman parte de muchos circuitos integrados o dispositivos electrónicos, el método de esta invención se centra fundamentalmente en ellas, pero pueden emplearse otros tipos de celdas de memoria estáticas.

Para probar las ventajas del método de la invención en aplicaciones de identificación/autenticación y generación de claves o secretos se han medido los valores a los que se estabilizan 168 celdas de memoria de una SRAM incluida en un circuito integrado de aplicaciones específicas fabricado en una tecnología de 90 nm de TSMC (Taiwan Semiconductor Manufacturing Company). La memoria no se ha desconectado del resto de la circuitería. Se han analizado 20 muestras del mismo circuito integrado en distintas condiciones de operación: tensión de alimentación de 0.9Vdd, Vdd y 1.1Vdd, con Vdd el valor de alimentación nominal; y temperaturas de 5ºC, 25ºC y 75ºC. Por cada condición de operación se han repetido 20 veces las medidas (con 20 veces ya se estabilizaba la clasificación resultante). La Figura 3 muestra en trazo negro continuo el porcentaje de celdas para las 20 muestras del circuito que se estabilizan siempre al mismo valor en todas las condiciones de operación si no se aplica el método de la invención.

Si se aplica la primera fase del método de la invención considerando los tres valores de tensión de alimentación (0.9Vdd, Vdd, y 1.1Vdd) a la misma temperatura (25ºC en ese caso), el porcentaje de celdas que se etiqueta como A se sitúa entre el 71.4% y el 83.9%. El porcentaje de esas celdas para las 20 muestras del circuito que se estabilizan siempre al mismo valor en todas las condiciones de operación (considerando el resto de temperaturas) se muestra en trazo gris continuo en la Figura 3. Al considerar sólo las celdas etiquetadas como A, el porcentaje de ellas que siempre proporciona el mismo valor ha aumentado considerablemente, pasando, por ejemplo en una de las muestras, del 73.8%, si no se aplica el método, al 90.5%, cuando se aplica el método.

Otra prueba realizada ha sido aplicar tres veces la primera fase del método considerando sólo el valor de tensión de alimentación nominal. La primera vez se realizó cuando la temperatura de operación del circuito era de 25ºC. Posteriormente se repite la primera fase del método cuando el circuito se encontraba a una temperatura de operación de 5ºC, y, de nuevo se repite la primera fase del método cuando el circuito se encontraba a una temperatura de operación de 75ºC. El porcentaje de celdas que se etiqueta como A se sitúa entre el 62.5% y el 73.8%. Las celdas etiquetadas como A son bastante más estables en todas las condiciones de operación. El porcentaje de esas celdas para las 20 muestras del circuito que se estabilizan siempre al mismo valor en todas las condiciones de operación (considerando el resto de tensiones de alimentación) se muestra en trazo discontinuo en la Figura 3. Al considerar sólo las celdas etiquetadas como A, el porcentaje de ellas que siempre proporciona el mismo valor ha aumentado de nuevo considerablemente, pasando, por ejemplo en una de las muestras, del 73.8%, si no se aplica el método, al 99.2%, cuando se aplica el método.

Para generar el identificador de n bits en la segunda fase del método, se necesitan n celdas etiquetadas como A. Si, en el peor caso, las celdas tipo A son el 62.5% de las N, se necesitan etiquetar del orden de 1.6n celdas al menos. Por ejemplo, para un identificador de 128 bits, se necesita que $N \geq 205$ celdas. El número de celdas N analizadas en la primera fase fija el tamaño máximo en bits de los identificadores que pueden generarse. Por supuesto, según la aplicación, puede generarse un identificador con más bits o varios identificadores con menos bits cada uno. El último caso puede ser interesante para cambiar el identificador que se genera, por ejemplo para revocar identificadores que pudieran haber sido comprometidos.

La Figura 4 ilustra cómo la aplicación del método de la invención mejora la separación entre la población impostora y genuina en aplicaciones de identificación/autenticación. Las gráficas corresponden a IDs de 128 bits. En trazo negro continuo se muestran las poblaciones resultantes cuando se usan 128 celdas cualesquiera de la memoria. En trazo gris continuo se muestran las poblaciones resultantes cuando se aplica el método con una primera fase considerando los tres valores de tensión de alimentación (0.9Vdd, Vdd, y 1.1Vdd) a la misma temperatura (25ºC) y el ID se genera con 128 celdas etiquetadas como A. En trazo discontinuo se muestran las poblaciones resultantes cuando se aplica el método, aplicando tres veces la primera fase considerando sólo el valor de tensión de alimentación nominal (la primera vez cuando la temperatura de operación del circuito era de 25ºC, posteriormente se repite para 5ºC, y, de nuevo se repite para 75ºC) y el ID se genera con 128 celdas etiquetadas como A. En las aplicaciones de identificación/autenticación hay que volver a registrar el ID de la memoria si se repite la primera fase del método.

Los resultados son ventajosos no sólo para generar IDs sino también para recuperar secretos o claves. Por ejemplo, la Figura 4 ilustra que la máxima distancia de Hamming entre IDs obtenidos en la fase de recuperación de clave e IDs registrados para un mismo conjunto de celdas (población genuina) puede llegar al 22% si no se aplica el método, que equivale al porcentaje de error que tendría que corregir el código corrector de errores en un algoritmo HDA. Aplicando la primera fase del método una vez contemplando diferentes tensiones de alimentación y la misma temperatura, la máxima distancia se reduce al 15%, lo que simplifica considerablemente el decodificador del código corrector de errores. Si la primera fase del método se realiza tres veces contemplando tres temperaturas de operación diferentes y la misma tensión de alimentación, según se ha comentado anteriormente, la fiabilidad de la generación de claves se incrementa (la máxima distancia de Hamming se reduce hasta el 10%).

Para probar las ventajas del método de la invención para generar números verdaderamente aleatorios se han medido los valores a los que se estabilizan 2280 celdas de memoria de la misma SRAM anterior incluida en un circuito integrado de aplicaciones específicas (fabricado en la tecnología de 90 nm de TSMC). Se han analizado 4 muestras del mismo circuito integrado en distintas condiciones de operación: tensión de alimentación de 0.9Vdd, Vdd y 1.1Vdd, con Vdd el valor de alimentación nominal; y temperaturas de 5ºC, 25ºC y 75ºC. Por cada condición de operación se han repetido 100 veces las medidas para obtener una buena estimación de la entropía. La Figura 5 muestra la entropía mínima total para las 4 muestras del

circuito medida en (a) condiciones nominales, (b) el peor caso para condiciones en que varíe la tensión de alimentación y (c) el peor caso para condiciones en que varíe la temperatura de operación. En todas las figuras, se muestra en trazo negro continuo la entropía mínima total medida cuando se consideran las 2280 celdas de memoria, sin aplicar el método de la invención. Se obtiene un peor valor del 1.7%.

En trazo gris continuo, la Figura 5 muestra la entropía mínima total medida cuando se consideran las celdas etiquetadas como B tras aplicar la primera fase del método de la invención considerando los tres valores de tensión de alimentación (0.9Vdd, Vdd, y 1.1Vdd) a la misma temperatura (25ºC en ese caso). El peor valor obtenido se incrementa hasta el 7.75%. El porcentaje de celdas que se etiqueta como B se sitúa entre 8.9% y el 10%. En trazo discontinuo se muestra la entropía mínima total medida cuando se consideran las celdas etiquetadas como B tras aplicar la primera fase del método tres veces considerando el valor de tensión nominal y las tres temperaturas de operación de 5ºC, 25ºC y 75ºC, como se comentó anteriormente. El peor valor obtenido de entropía mínima total se incrementa hasta el 16%. El porcentaje de celdas que se etiqueta como B se reduce, situándose entre el 2.6% y el 3.8%.

Para generar un número aleatorio de m bits, se necesitan m celdas etiquetadas como B. Si, en el peor caso, las celdas tipo B son el 8.9% de las N, se necesitan etiquetar del orden de 11.2m celdas al menos. Por ejemplo, para generar un número aleatorio de 80 bits, se necesita que N ≥ 896 celdas. Si se ha refinado más la clasificación y, en el peor caso, las celdas tipo B son el 2.6% de las N, se necesitan etiquetar del orden de 38.5m celdas al menos. Por ejemplo, para generar un número aleatorio de 80 bits, se necesita que N ≥ 3080 celdas. El número de celdas N analizadas en la primera fase fija el tamaño máximo en bits de los números verdaderamente aleatorios que pueden generarse. Normalmente esto no es una limitación porque las memorias estáticas que se emplean en los dispositivos electrónicos actuales son de elevada capacidad. Por supuesto, según la aplicación, puede generarse un número aleatorio con más bits o varios números aleatorios con menos bits cada uno.

El tiempo que se ha elegido en los experimentos para dejar sin alimentación la memoria ha sido de 30 segundos. Si en la primera fase del método se realizan Q=20 medidas por cada P=3 tensión de alimentación, son necesarios 30x20x3=1800 segundos = 30 minutos. En cada medida hay que leer las N celdas de memoria, pero este tiempo es despreciable frente al anterior, por lo que pueden analizarse muchas

celdas. La primera fase del método puede realizarse en cualquier intervalo de tiempo en el que no se necesite generar identificadores o números aleatorios. Además, no es una fase que tenga que realizarse continuamente. Por otro lado, el tiempo para generación de números viene marcado fundamentalmente por el tiempo de lectura de las celdas necesarias para generar el identificador de n bits y el número aleatorio de m bits. La memoria analizada en los experimentos proporcionaba 60 bits por cada palabra y el tiempo de lectura de cada palabra era al menos 2.4 nanosegundos. En el peor de los casos (que cada celda tuviera direcciones de acceso diferentes) para generar un número de n bits se necesitarían 2.4 nanosegundos por cada bit, por ejemplo 307.2 nanosegundos para un número de 128 bits. Si la memoria analizada es de doble puerto, el tiempo se reduce a la mitad: 1.2 nanosegundos por cada bit en el peor caso, por ejemplo 153.6 nanosegundos para un número de 128 bits. El método de la invención no solo reduce el tiempo de lectura de celdas (porque se necesitan leer menos celdas) sino también el tiempo del posible procesado posterior (por ejemplo, si se aplicara una función hash para obtener una semilla completamente aleatoria de 128 bits en todas las condiciones de operación, se necesitarían procesar 942 bytes sin aplicar el método, mientras que solo se necesitarían procesar 207 bytes tras aplicar el método con una primera fase contemplando tres valores de tensión de alimentación, como se comentó anteriormente, lo que significaría una reducción en el procesado de datos del 78%).

El método puede implementarse mediante un dispositivo que presenta al menos dos modos de operación seleccionables: modo de etiquetado de celdas de memoria y modo de generación de números, donde el modo de generación de números funciona correctamente si previamente se ha llevado a cabo el modo de etiquetado al menos una vez. Dicho dispositivo está caracterizado porque comprende:

- una memoria estática (1),
- un bloque de tensión (2) que deja de alimentar a la memoria (1) o la alimenta a un valor de tensión determinado,
- un bloque de clasificación (3) que, si el modo de operación es el de etiquetado, analiza a qué celdas de la memoria (1) asignarles la etiqueta A y a cuáles la etiqueta B, y, si el modo de operación es el de generación de números, envía el resultado de la clasificación al bloque de control (4);
- un bloque de control (4) que controla todos los demás bloques para ejecutar los pasos del método, de modo que: (a) indica al bloque de tensión (2) cuándo no alimentar a la memoria (1) y cuándo alimentarla y, en tal caso, fija el valor de la

tensión de alimentación; (b) habilita la lectura de la memoria (1) y activa las señales específicas de la lectura de las celdas de memoria; (c) indica al bloque de clasificación (3) el modo de operación y, si el modo de operación es el de generación de números, (d) emplea la información almacenada del modo de etiquetado para leer los bits generados por las celdas de memoria con etiqueta A y generar con ellos identificadores y los bits generados por las celdas con etiqueta B y generar con ellos números aleatorios.

La Figura 6 muestra el diagrama de bloques del dispositivo que implementa el método de la invención.

En una realización del dispositivo, la memoria estática (1) es una memoria estática de acceso aleatorio, SRAM.

El bloque de tensión puede realizarse mediante una fuente de alimentación programable de las que se dispone en muchos laboratorios. Sin embargo, para conseguir una realización portable y barata que pueda, por ejemplo, incluirse en la placa de circuito impreso que contenga la memoria, es preferible que el bloque de tensión (2) comprenda:

- un interruptor controlado por una señal digital del bloque de control (4) que cierra o abre el interruptor para alimentar o no a la memoria (1) y
- un potenciómetro controlado digitalmente por el bloque de control (4) para modificar el valor de la tensión que alimenta a la memoria (1), en el caso de analizar más de un valor de tensión de alimentación (en el caso de analizar solo el valor de tensión nominal no es necesario el potenciómetro).

En una realización preferente del dispositivo, el bloque de clasificación (3) comprende:

- una memoria o registros para almacenar los N bits leídos de la memoria (1) en la primera medida realizada a una tensión de alimentación, borrándose los anteriormente almacenados;
- operadores XOR destinados a comparar los bits leídos de la memoria (1) en cada medida con los bits almacenados de la primera medida realizada al mismo valor de tensión de alimentación, resultando valores lógicos “0” si los valores de los bits de ambas lecturas coinciden y valores “1” si los valores no coinciden;

- operadores OR destinados a ir combinando los resultados de los operadores XOR anteriores obtenidos sobre medidas al mismo valor de tensión de alimentación, resultando un valor lógico "0" para una celda que siempre va proporcionando el mismo valor de bit en todas las medidas y un valor lógico "1" para una celda que alguna vez haya proporcionado un valor de bit diferente;
- una memoria o registros destinados a almacenar NxP bits (N bits por cada uno de los P valores de tensión de alimentación analizados), cada bit de los N etiquetando una de las N celdas de memoria analizadas, de modo que el valor del bit indica si la celda ha sido etiquetada como S (valor del bit "0") o como U (valor del bit "1") para cada valor de tensión, de modo que, en el caso de analizar un único valor de tensión, a una celda etiquetada como S se le asigna el código de la etiqueta A y a una celda etiquetada como U se le asigna el código de la etiqueta B;
- operadores NOR, en el caso de analizar P>1 valores de tensión de alimentación, destinados a combinar P bits de etiquetas por cada celda, de forma que si resulta un valor lógico "1", a la celda se le asigna el código de la etiqueta A;
- operadores AND, en el caso de analizar P>1 valores de tensión de alimentación, destinados a combinar P bits de etiquetas por cada celda, de forma que si resulta un valor lógico "1", a la celda se le asigna el código de la etiqueta B;
- una memoria o registros para almacenar 2N bits, en el caso de analizar P>1 valores de tensión de alimentación, cada 2 bits codificando si cada una de las N celdas de memoria analizadas posee la etiqueta A, B ó ninguna de ellas.
- operadores XOR destinados a comparar las etiquetas asociadas a las N celdas obtenidas en el modo de operación de etiquetado actual con las etiquetas obtenidas en modo(s) de operación de etiquetado anteriores.

Por supuesto, cualquier otra realización equivalente a la anteriormente descrita sería igualmente válida (por ejemplo, aplicando que operadores NAND de datos complementados es equivalente a operadores OR de datos sin complementar).

Las memorias o registros empleados por el bloque de clasificación pueden borrarse o re-escribirse tras el modo de etiquetado, salvo la memoria o registros que almacenan

los 2N bits de las etiquetas, que deben mantenerse para ser empleados en el modo de generación de números del dispositivo o en posibles repeticiones del etiquetado.

En una realización preferente del dispositivo, el bloque de control (4) comprende:

- contadores para medir: (a) el tiempo que se deja al bloque de memoria (1) sin alimentar, (b) las medidas que se llevan a cabo por cada valor de tensión de alimentación, (c) el número de los valores de tensión a analizar, en el caso de analizar varias tensiones de alimentación, (d) las celdas de memoria que se analizan, (e) el número de bits para generar identificadores y (f) el número de bits para generar números aleatorios;
- un bloque que traduce en direcciones de acceso a la memoria (1) las etiquetas asociadas a las N celdas.

Como las etiquetas asociadas a las celdas se almacenan en orden se puede saber cómo acceder a las celdas etiquetadas como A para generar los identificadores y a las etiquetadas como B para generar los números aleatorios (se sabe, por ejemplo, a qué palabra de la memoria corresponden y a qué bit dentro de la palabra).

Al configurar en el dispositivo el modo de operación de etiquetado, el bloque de control (4) recibe como parámetros de configuración al menos el número N de celdas de memoria a analizar, el número P de tensiones de alimentación a fijar, el número Q de medidas a realizar por cada tensión de alimentación y una señal binaria REP, que indica si se repite el etiquetado o no, y recibe una señal de inicio, INIT, que inicializa a cero todos los contadores y que marca el comienzo del proceso de etiquetado, de modo que el bloque de control (4), para cada una de las tensiones a analizar, indica al bloque de tensión (2) que no alimente la memoria (1) durante el tiempo necesario, que está controlado por uno de los contadores del bloque de control; transcurrido ese tiempo, el bloque de control (4) indica al bloque de tensión (2) que alimente la memoria (1) al valor de tensión determinado y activa las señales específicas de la lectura de datos en la memoria (1) para leer los bits a los que se han estabilizado N celdas de memoria, dependiendo el mecanismo de lectura de las señales de entrada y de la memoria (1), dependiendo la temporización de dicha lectura del tipo de memoria empleada, y controlando uno de los contadores del bloque de control (4) cuándo se finaliza la lectura de N celdas al menos; además, el bloque de control (4) indica al bloque de clasificación (3) que opere en modo de etiquetado, de manera que el bloque de clasificación (3) recibe los N bits de la memoria (1), almacenando los bits

correspondientes a la primera medida de cada tensión de alimentación y comparando con ellos los sucesivos N bits leídos en las sucesivas medidas, empleando operadores XOR para la comparación, y combinando con operadores OR los resultados para cada celda obtenidos de las operaciones XOR, resultando un valor lógico "0" para las celdas que siempre proporcionan el mismo valor de bit en las sucesivas medidas y un valor lógico "1" para las celdas que han cambiado alguna vez el valor de bit proporcionado en las sucesivas medidas, almacenando esos resultados en una memoria o registros de N bits asociados con la tensión de alimentación analizada; de modo que cuando el contador del bloque de control (4) que cuenta las medidas analizadas a ese valor de tensión llega al valor de cuenta Q configurado, si P=1 y REP=0 (el etiquetado no se repite), el bloque de control (4) indica al bloque de clasificación (3) que almacene en una memoria o registros de 2N bits, de forma ordenada, las N etiquetas codificadas con 2 bits de las N celdas, de forma que el bloque de clasificación (3) almacena los 2 bits que indican la etiqueta A para las celdas que siempre proporcionaron el mismo valor de bit (resultaron un valor lógico "0" tras la operación OR) y almacena los 2 bits que indican la etiqueta B para las celdas que cambiaron alguna vez el valor de bit proporcionado (resultaron un valor lógico "1" tras la operación OR); y si REP=1 y N mantiene su valor (el etiquetado se repite), el bloque de control (4) indica al bloque de clasificación (3) que compare de forma ordenada y mediante operadores XOR si cada etiqueta obtenida para cada celda es A ó B, como en etiquetados anteriores, en cuyo caso se mantienen almacenadas en la memoria o registros de 2N bits las correspondientes etiquetas A ó B, mientras que si la nueva etiqueta obtenida no es ni A ni B o no coinciden con las anteriores las nuevas etiquetas obtenidas, entonces se almacenan para esa celda 2 bits que indican la etiqueta C; mientras que si P>1, el bloque de control (4) inicia otras Q medidas, inicializando los contadores que cuentan el número de celdas a analizar y el número de medidas a realizar, indicando al bloque de tensión (2) el siguiente valor de tensión a analizar; repitiéndose el proceso hasta que el contador del bloque de control (4) que cuenta los valores de tensión analizados llega al valor de cuenta P configurado, en cuyo caso, el bloque de control (4) indica al bloque de clasificación (3) que combine los P grupos de N bits almacenados para cada tensión de alimentación analizada mediante operadores NOR y AND y almacene en una memoria o registros de 2N bits, de forma ordenada, las N etiquetas codificadas con 2 bits de las N celdas, de forma que el bloque de clasificación (3), si REP=0, almacena los 2 bits que indican la etiqueta A para las celdas que siempre proporcionaron el mismo valor de bit para todas las medidas y todas las tensiones (resultaron un valor lógico "1" tras la operación

NOR), almacena los 2 bits que indican la etiqueta B para las celdas que cambiaron alguna vez el valor de bit proporcionado para todas las tensiones (resultaron un valor lógico "1" tras la operación AND), y almacena 2 bits que indican la etiqueta C, para el resto de las celdas, y si REP=1 y el valor de N se mantiene, el bloque de control (4) indica al bloque de clasificación (3) que compare de forma ordenada y mediante operadores XOR si cada etiqueta obtenida para cada celda es A ó B, como en etiquetados anteriores, en cuyo caso se mantienen almacenadas en la memoria o registros de 2N bits las correspondientes etiquetas A ó B, mientras que si la nueva etiqueta obtenida no es ni A ni B o no coinciden con las anteriores las nuevas etiquetas obtenidas, se almacenan para esa celda los 2 bits que indican la etiqueta C; de forma que, cuando el proceso de etiquetado ha finalizado, el bloque de control (4) lo indica mediante una señal binaria FIN.

Al configurar en el dispositivo el modo de operación de generación de números, el bloque de control (4) recibe como parámetros de configuración al menos el tamaño en bits, n, del identificador a generar y el tamaño en bits, m, del número aleatorio a generar, y recibe una señal de inicio, INIT, que inicializa a cero todos los contadores y marca el comienzo del proceso de generación, de modo que el bloque de control (4) indica al bloque de tensión (2) que no alimente la memoria (1) durante el tiempo necesario, que está controlado por uno de los contadores del bloque de control; transcurrido ese tiempo (o bien si la memoria ya llevaba al menos ese tiempo desconectada de la alimentación) el bloque de control (4) indica al bloque de tensión (2) que alimente la memoria al valor de tensión nominal e indica al bloque de clasificación (3) que le envíe las etiquetas asociadas a las N celdas, de modo que son traducidas a direcciones de acceso a las celdas de tipo A y B de la memoria (1); empleando esa información, el bloque de control activa las señales específicas de la lectura de datos en las celdas de tipo A y B de la memoria (1), dependiendo el mecanismo de lectura de las señales de entrada y de la memoria (1) y dependiendo la temporización de dicha lectura del tipo de memoria empleada, y el bloque de control (4) concatena los bits generados por celdas etiquetadas como A en la cadena-A y los bits generados por celdas etiquetadas como B en la cadena-B; de forma que uno de los contadores del bloque de control cuenta n bits de la cadena-A, que el bloque de control los proporciona como identificador y uno de los contadores del bloque de control cuenta m bits de la cadena-B, que el bloque de control los proporciona como número verdaderamente aleatorio; de manera que, cuando el proceso de generación

de números ha finalizado, el bloque de control (4) lo indica mediante una señal binaria FIN.

Modo de realización de la invención

La funcionalidad de los bloques de clasificación y de control puede realizarse mediante un software ejecutado en un microcontrolador o microprocesador para el que la memoria sea una memoria externa.

Otra posibilidad es realizar mediante circuitería adicional (hardware dedicado) los bloques de clasificación y de control. La Figura 7 ilustra un esquemático de esta solución. Los bloques de clasificación y de control se han implementado en una FPGA (Field Programmable Gate Array) XC3S50 de Xilinx, que dispone de 1728 celdas lógicas equivalentes y 72 Kbits (K=1024) de Block RAMs (4 Block RAMs de 18 Kbits cada una). Este ejemplo de realización incluye una memoria estática SRAM, externa a la FPGA, con capacidad para 2^{15} palabras de 8 bits cada una, que permite la lectura en paralelo de los 8 bits. El bloque de tensión, también externo a la FPGA, contiene un potenciómetro controlado mediante una señal de 11 bits y un interruptor controlado mediante una señal de 1 bit, donde los 12 bits de control los proporciona el bloque de control implementado mediante una máquina de estados finitos (FSM) en la FPGA. Tanto la FPGA como el bloque de tensión reciben la alimentación externamente a través de un regulador de tensión mientras que la SRAM recibe la alimentación del bloque de tensión. Todo se incluye en una placa de circuito impreso de reducidas dimensiones.

En este ejemplo de realización, la SRAM no forma parte de ningún sistema digital pero en otras realizaciones, la SRAM podría ser un bloque de un sistema mayor y no sería necesario desconectarla del sistema.

La FSM (bloque de control) implementada en la FPGA controla, mediante la señal binaria "Modo" (que toma el valor que se le indique a la entrada), si el modo de operación es de generación de números (en cuyo caso los bits que se leen de la SRAM se envían al bloque de control) o el modo es de etiquetado (en cuyo caso los bits que se leen se envían al bloque de clasificación).

En el modo de operación de etiquetado, la FSM (bloque de control) controla todas las señales de habilitación de escritura y lectura de las Block RAMs de la FPGA y toda la temporización de los pasos del etiquetado. La FSM contiene un contador de 32 bits para medir el tiempo que se deja al bloque de memoria sin alimentar. Este contador tiene el tamaño necesario para contar al menos 30 segundos a la frecuencia de reloj de la FPGA (que es de 50MHz) sin llegar a desbordarse. La FSM contiene también un contador de 5 bits para contar las medidas, Q, que se llevan a cabo por cada valor de tensión de alimentación (que toma el valor que se le indica a la entrada) y un contador de 2 bits para contar el número, P, de los valores de tensión a analizar (que toma el valor que se le indica a la entrada, limitado en este ejemplo de realización a 3 valores). La FSM también controla si la medida que se realiza de la memoria es la primera de una fase de etiquetado o no. Los bits que se leen por primera vez de la SRAM se almacenan en una de las Block RAMs de la FPGA y los bits de las medidas sucesivas se van comparando con ellos mediante operadores XOR (8 operadores XOR en esta realización para comparar los 8 bits de una palabra en paralelo). Los resultados (etiquetas S ó U) para los tres valores de tensión de alimentación posibles de este ejemplo se almacenan en las otras tres Block RAMs. Las etiquetas finales del proceso de etiquetado (etiquetas A, B ó C) se almacenan en la primera de las Block RAMs. Como se dejan N bits libres de esa Block RAM para guardar las primeras medidas de otros posibles etiquetados, se pueden almacenar en este ejemplo de realización las etiquetas de hasta N= 6144 celdas ocupando toda esa Block RAM. La FSM contiene un contador de 10 bits para contar las N celdas de memoria a analizar (hasta 2^{10} x 8 celdas, pero con el límite en 6144 celdas). El contador de 10 bits realiza la función de direccionar la memoria. Si la señal REP (que toma el valor que se le marca a la entrada) indica que se repita el etiquetado y el valor de N se mantiene, las nuevas etiquetas (A, B ó C) obtenidas se comparan mediante operadores XOR con las anteriormente almacenadas, de forma que si la salida de dichos operadores indica que no ha habido cambio de etiquetado, las etiquetas almacenadas se mantienen mientras que si ha habido cambio, se almacena la etiqueta C. Este control de etiquetado es el que realiza el sub-bloque denominado "lógica de etiquetado" dentro del bloque de clasificación.

Cuando el modo seleccionado es el de generación de números, el contador de 10 bits de la FSM también realiza la función de direccionar la memoria. El sub-bloque "traductor de etiquetas" que contiene la FSM comprueba si en la palabra que direcciona el contador existe un bit que vaya a utilizarse para generar un identificador

o un número verdaderamente aleatorio. En caso afirmativo, la FSM lee esa palabra de la SRAM y selecciona los bits para el identificador o el número aleatorio en función de su etiqueta. Si no fuera así, el contador se incrementa sin que se lea esa palabra. Un contador de 7 bits cuenta el número de bits, n, de los identificadores y el número de bits, m, de los números aleatorios. En este ejemplo de realización, los bits del identificador y del número verdaderamente aleatorio se proporcionan en serie por las salidas ID y TRN, respectivamente.

Según el modo de operación, los 7 bits por el bus de entrada n/P se toman como valor de n (modo de generación de números) o P (modo de etiquetado) y los 7 bits por el bus de entrada m/Q se toman como valor de m (modo de generación de números) o Q (modo de etiquetado). Los 10 bits por el bus de entrada N permiten elegir el número de direcciones que se leen como máximo de la memoria, mientras que las señales binarias INIT, REP y FIN indican, respectivamente, el inicio del procesado, si hay o no repetición del modo etiquetado y la finalización del procesado.

Reivindicaciones

1.- Método para generar al menos un número de identificación de n bits y al menos un número verdaderamente aleatorio de m bits a partir de N celdas de memoria estáticas teniendo cada celda capacidad de almacenar un bit de información, en el cual n puede tomar valores desde 0 hasta N-m y m puede tomar valores desde 0 hasta N-n,

estando el método caracterizado porque comprende una primera fase en la que se clasifican las N celdas de memoria en al menos dos grupos etiquetados como A y B, y una segunda fase en la que se generan al menos un número de identificación de n bits a partir de n celdas etiquetadas en la primera fase como A y al menos un número verdaderamente aleatorio de m bits a partir de m celdas etiquetadas en la primera fase como B, donde la primera fase de clasificación se lleva a cabo al menos una vez, de forma que, una vez clasificadas las celdas, la generación de números de identificación y aleatorios se puede llevar a cabo directamente ejecutando la segunda fase sin tener que volver a ejecutar la primera fase;

donde la primera fase del método a su vez comprende:

(a) dejar sin alimentación a la memoria (y, por tanto, a sus celdas) durante un tiempo suficiente para que desaparezcan todos los valores de los bits que pudieran estar almacenados,

(b) conectar la memoria a una tensión de alimentación fijada y leer los valores de los bits a los que se han estabilizado N celdas de memoria sin antes haber escrito nada en ellas,

(c) guardar los valores de los bits leídos de las N celdas,

(d) dejar sin alimentación a la memoria durante el tiempo suficiente para borrar los valores almacenados,

(e) alimentar de nuevo la memoria con el mismo valor de tensión y volver a leer los valores de bits de las N celdas sin antes haber escrito nada en ellas,

(f) comparar los valores de bits obtenidos en el paso (e) con los guardados en el paso (c), clasificando las celdas de memoria en dos grupos: las celdas que siempre proporcionan el mismo valor de bit y las celdas que alguna vez han proporcionado un valor de bit diferente,

(g) ir al paso (h) si ya se han tomado todas las medidas para el mismo valor de tensión de alimentación fijado; mientras que, en otro caso, volver al paso (d),

(h) etiquetar las celdas que siempre han proporcionado el mismo valor de bit para todas las medidas realizadas a un mismo valor de tensión como S, etiquetar las otras celdas como U y guardar el resultado de la clasificación para el valor de tensión analizada,

(i) ir al paso (j) si ya se han analizado todos los valores de tensión de alimentación; mientras que, en otro caso, fijar un nuevo valor de tensión de alimentación a analizar y volver al paso (a),

(j) comparar los resultados de clasificación obtenidos para los valores de tensión analizados y etiquetar las celdas de memoria que han sido etiquetadas siempre como S con todos los valores de tensión analizados con una etiqueta A y etiquetar las celdas que han sido etiquetadas siempre como U con todos los valores de tensión analizados con una etiqueta B (asignando una etiqueta C a las celdas que no se les asigna una etiqueta A ni B);

y donde la segunda fase del método a su vez comprende:

(1) dejar sin alimentación a la memoria (y, por tanto, a sus celdas) durante un tiempo suficiente para que desaparezcan todos los valores de bits que pudieran estar almacenados,

(2) alimentar la memoria a su valor de tensión nominal, no escribir nada en las N celdas analizadas en la primera fase y generar una secuencia de bits (cadena-A) con los valores de bits a los que se hayan estabilizado las celdas etiquetadas como A y generar otra secuencia de bits (cadena-B) con los valores de bits de las celdas etiquetadas como B, finalizando la lectura cuando al menos se tenga una cadena-A de n bits y una cadena-B de m bits,

(3) utilizar la cadena-A para generar al menos un número de identificación digital de n bits y la cadena-B para generar al menos un número verdaderamente aleatorio de m bits.

2. Método según la reivindicación 1 caracterizado porque en una primera fase se analizan P valores de tensión de alimentación (siendo P mayor o igual a 1), de los cuales al menos uno es el valor de tensión nominal (Vdd).

3. Método según una cualquiera de las reivindicaciones 1 a 2, caracterizado porque al repetirse la primera fase del método, se etiquetan con una etiqueta A las celdas que en la anterior primera fase se etiquetaron con A y en la actual primera fase del método vuelven a etiquetarse como A; se etiquetan con una etiqueta B las celdas que en la anterior primera fase se etiquetaron con B y en la actual primera fase del método vuelven a etiquetarse como B y se etiquetan con una etiqueta C el resto de las celdas.

4.- Método según una cualquiera de las reivindicaciones 1 a 2, caracterizado porque al realizarse la primera fase del método sin indicar que sea una repetición, se borra cualquier resultado de posibles clasificaciones anteriores y se almacena el resultado de la clasificación actual.

5. Dispositivo para implementar el método según se define en las reivindicaciones 1 a 4 que presenta al menos dos modos de operación seleccionables: modo de etiquetado de celdas de memoria y modo de generación de números, donde el modo de generación de números funciona correctamente si previamente se ha llevado a cabo el modo de etiquetado al menos una vez; estando dicho dispositivo caracterizado porque comprende:

- una memoria estática (1),
- un bloque de tensión (2) que deja de alimentar a la memoria (1) o la alimenta a un valor de tensión determinado,
- un bloque de clasificación (3) que, si el modo de operación es el de etiquetado, analiza a qué celdas de la memoria (1) asignarles la etiqueta A y a cuáles la etiqueta B, y, si el modo de operación es el de generación de números, envía el resultado de la clasificación al bloque de control (4);
- un bloque de control (4) que controla todos los demás bloques para ejecutar los pasos del método, de modo que: (a) indica al bloque de tensión (2) cuándo no alimentar a la memoria (1) y cuándo alimentarla y, en tal caso, fija el valor de la

tensión de alimentación; (b) habilita la lectura de la memoria (1) y activa las señales específicas de la lectura de las celdas de memoria; (c) indica al bloque de clasificación (3) el modo de operación y, si el modo de operación es el de generación de números, (d) emplea la información almacenada del modo de etiquetado para leer los bits generados por las celdas de memoria con etiqueta A y generar con ellos identificadores y los bits generados por las celdas con etiqueta B y generar con ellos números aleatorios.

6. Dispositivo según reivindicación 5 caracterizado porque la memoria estática (1) es una memoria estática de acceso aleatorio, SRAM.

7. Dispositivo según cualquiera de las reivindicaciones 5 a 6 caracterizado porque el bloque de tensión (2) comprende:

- un interruptor controlado por una señal digital del bloque de control (4) que cierra o abre el interruptor para alimentar o no a la memoria (1) y
- un potenciómetro controlado digitalmente por el bloque de control (4) para modificar el valor de la tensión que alimenta a la memoria (1), en el caso de analizar más de un valor de tensión de alimentación (en el caso de analizar solo el valor de tensión nominal no es necesario el potenciómetro).

8. Dispositivo según cualquiera de las reivindicaciones 5 a 7 caracterizado porque el bloque de clasificación (3) comprende:

- una memoria o registros para almacenar los N bits leídos de la memoria (1) en la primera medida realizada a una tensión de alimentación, borrándose los anteriormente almacenados;
- operadores XOR destinados a comparar los bits leídos de la memoria (1) en cada medida con los bits almacenados de la primera medida realizada al mismo valor de tensión de alimentación, resultando valores lógicos “0” si los valores de los bits de ambas lecturas coinciden y valores “1” si los valores no coinciden;
- operadores OR destinados a ir combinando los resultados de los operadores XOR anteriores obtenidos sobre medidas al mismo valor de tensión de

alimentación, resultando un valor lógico "0" para una celda que siempre va proporcionando el mismo valor de bit en todas las medidas y un valor lógico "1" para una celda que alguna vez haya proporcionado un valor de bit diferente;

- una memoria o registros destinados a almacenar NxP bits (N bits por cada uno de los P valores de tensión de alimentación analizados), cada bit de los N etiquetando una de las N celdas de memoria analizadas, de modo que el valor del bit indica si la celda ha sido etiquetada como S (valor del bit "0") o como U (valor del bit "1") para cada valor de tensión, de modo que, en el caso de analizar un único valor de tensión, a una celda etiquetada como S se le asigna el código de la etiqueta A y a una celda etiquetada como U se le asigna el código de la etiqueta B;
- operadores NOR, en el caso de analizar P>1 valores de tensión de alimentación, destinados a combinar P bits de etiquetas por cada celda, de forma que si resulta un valor lógico "1", a la celda se le asigna el código de la etiqueta A;
- operadores AND, en el caso de analizar P>1 valores de tensión de alimentación, destinados a combinar P bits de etiquetas por cada celda, de forma que si resulta un valor lógico "1", a la celda se le asigna el código de la etiqueta B;
- una memoria o registros para almacenar 2N bits, en el caso de analizar P>1 valores de tensión de alimentación, cada 2 bits codificando si cada una de las N celdas de memoria analizadas posee la etiqueta A, B ó ninguna de ellas.
- operadores XOR destinados a comparar las etiquetas asociadas a las N celdas obtenidas en el modo de operación de etiquetado actual con las etiquetas obtenidas en modo(s) de operación de etiquetado anteriores.

9. Dispositivo según cualquiera de las reivindicaciones 5 a 8 caracterizado porque el bloque de control (4) comprende:

- contadores para medir: (a) el tiempo que se deja al bloque de memoria (1) sin alimentar, (b) las medidas que se llevan a cabo por cada valor de tensión de alimentación, (c) el número de los valores de tensión a analizar, en el caso de analizar varias tensiones de alimentación, (d) las celdas de memoria que se analizan, (e) el número de bits para generar identificadores y (f) el número de bits para generar números aleatorios;

- un bloque que traduce en direcciones de acceso a la memoria (1) las etiquetas asociadas a las N celdas.

10. Dispositivo según cualquiera de las reivindicaciones 5 a 9 en el que, al configurar el modo de operación de etiquetado, el bloque de control (4) recibe como parámetros de configuración al menos el número N de celdas de memoria a analizar, el número P de tensiones de alimentación a fijar, el número Q de medidas a realizar por cada tensión de alimentación y una señal binaria REP, que indica si se repite el etiquetado o no, y recibe una señal de inicio, INIT, que inicializa a cero todos los contadores y que marca el comienzo del proceso de etiquetado, de modo que el bloque de control (4), para cada una de las tensiones a analizar, indica al bloque de tensión (2) que no alimente la memoria (1) durante el tiempo necesario, que está controlado por uno de los contadores del bloque de control; transcurrido ese tiempo, el bloque de control (4) indica al bloque de tensión (2) que alimente la memoria (1) al valor de tensión determinado y activa las señales específicas de la lectura de datos en la memoria (1) para leer los bits a los que se han estabilizado N celdas de memoria, dependiendo el mecanismo de lectura de las señales de entrada y de la memoria (1), dependiendo la temporización de dicha lectura del tipo de memoria empleada, y controlando uno de los contadores del bloque de control (4) cuándo se finaliza la lectura de N celdas al menos; además, el bloque de control (4) indica al bloque de clasificación (3) que opere en modo de etiquetado, de manera que el bloque de clasificación (3) recibe los N bits de la memoria (1), almacenando los bits correspondientes a la primera medida de cada tensión de alimentación y comparando con ellos los sucesivos N bits leídos en las sucesivas medidas, empleando operadores XOR para la comparación, y combinando con operadores OR los resultados para cada celda obtenidos de las operaciones XOR, resultando un valor lógico “0” para las celdas que siempre proporcionan el mismo valor de bit en las sucesivas medidas y un valor lógico “1” para las celdas que han cambiado alguna vez el valor de bit proporcionado en las sucesivas medidas, almacenando esos resultados en una memoria o registros de N bits asociados con la tensión de alimentación analizada; de modo que cuando el contador del bloque de control (4) que cuenta las medidas analizadas a ese valor de tensión llega al valor de cuenta Q configurado, si P=1 y REP=0 (el etiquetado no se repite), el bloque de control (4) indica al bloque de clasificación (3) que almacene en una memoria o registros de 2N bits, de forma ordenada, las N etiquetas codificadas con 2 bits de las N celdas, de forma que el bloque de clasificación (3) almacena los 2 bits que indican la etiqueta A para las celdas que siempre proporcionaron el mismo valor

de bit (resultaron un valor lógico "0" tras la operación OR) y almacena los 2 bits que indican la etiqueta B para las celdas que cambiaron alguna vez el valor de bit proporcionado (resultaron un valor lógico "1" tras la operación OR); y si REP=1 y N mantiene su valor (el etiquetado se repite), el bloque de control (4) indica al bloque de clasificación (3) que compare de forma ordenada y mediante operadores XOR si cada etiqueta obtenida para cada celda es A ó B, como en etiquetados anteriores, en cuyo caso se mantienen almacenadas en la memoria o registros de 2N bits las correspondientes etiquetas A ó B, mientras que si la nueva etiqueta obtenida no es ni A ni B o no coinciden con las anteriores las nuevas etiquetas obtenidas, entonces se almacenan para esa celda 2 bits que indican la etiqueta C; mientras que si P>1, el bloque de control (4) inicia otras Q medidas, inicializando los contadores que cuentan el número de celdas a analizar y el número de medidas a realizar, indicando al bloque de tensión (2) el siguiente valor de tensión a analizar; repitiéndose el proceso hasta que el contador del bloque de control (4) que cuenta los valores de tensión analizados llega al valor de cuenta P configurado, en cuyo caso, el bloque de control (4) indica al bloque de clasificación (3) que combine los P grupos de N bits almacenados para cada tensión de alimentación analizada mediante operadores NOR y AND y almacene en una memoria o registros de 2N bits, de forma ordenada, las N etiquetas codificadas con 2 bits de las N celdas, de forma que el bloque de clasificación (3), si REP=0, almacena los 2 bits que indican la etiqueta A para las celdas que siempre proporcionaron el mismo valor de bit para todas las medidas y todas las tensiones (resultaron un valor lógico "1" tras la operación NOR), almacena los 2 bits que indican la etiqueta B para las celdas que cambiaron alguna vez el valor de bit proporcionado para todas las tensiones (resultaron un valor lógico "1" tras la operación AND), y almacena 2 bits que indican la etiqueta C, para el resto de las celdas, y si REP=1 y el valor de N se mantiene, el bloque de control (4) indica al bloque de clasificación (3) que compare de forma ordenada y mediante operadores XOR si cada etiqueta obtenida para cada celda es A ó B, como en etiquetados anteriores, en cuyo caso se mantienen almacenadas en la memoria o registros de 2N bits las correspondientes etiquetas A ó B, mientras que si la nueva etiqueta obtenida no es ni A ni B o no coinciden con las anteriores las nuevas etiquetas obtenidas, se almacenan para esa celda los 2 bits que indican la etiqueta C; de forma que, cuando el proceso de etiquetado ha finalizado, el bloque de control (4) lo indica mediante una señal binaria FIN.

11. Dispositivo según cualquiera de las reivindicaciones 5 a 10 en el que, al configurar el modo de operación de generación de números, el bloque de control (4) recibe como parámetros de configuración al menos el tamaño en bits, n, del identificador a generar y el tamaño en bits, m, del número aleatorio a generar, y recibe una señal de inicio, INIT, que inicializa a cero todos los contadores y marca el comienzo del proceso de generación, de modo que el bloque de control (4) indica al bloque de tensión (2) que no alimente la memoria (1) durante el tiempo necesario, que está controlado por uno de los contadores del bloque de control; transcurrido ese tiempo (o bien si la memoria ya llevaba al menos ese tiempo desconectada de la alimentación) el bloque de control (4) indica al bloque de tensión (2) que alimente la memoria al valor de tensión nominal e indica al bloque de clasificación (3) que le envíe las etiquetas asociadas a las N celdas, de modo que son traducidas a direcciones de acceso a las celdas de tipo A y B de la memoria (1); empleando esa información, el bloque de control activa las señales específicas de la lectura de datos en las celdas de tipo A y B de la memoria (1), dependiendo el mecanismo de lectura de las señales de entrada y de la memoria (1) y dependiendo la temporización de dicha lectura del tipo de memoria empleada, y el bloque de control (4) concatena los bits generados por celdas etiquetadas como A en la cadena-A y los bits generados por celdas etiquetadas como B en la cadena-B; de forma que uno de los contadores del bloque de control cuenta n bits de la cadena-A, que el bloque de control los proporciona como identificador y uno de los contadores del bloque de control cuenta m bits de la cadena-B, que el bloque de control los proporciona como número verdaderamente aleatorio; de manera que, cuando el proceso de generación de números ha finalizado, el bloque de control (4) lo indica mediante una señal binaria FIN.

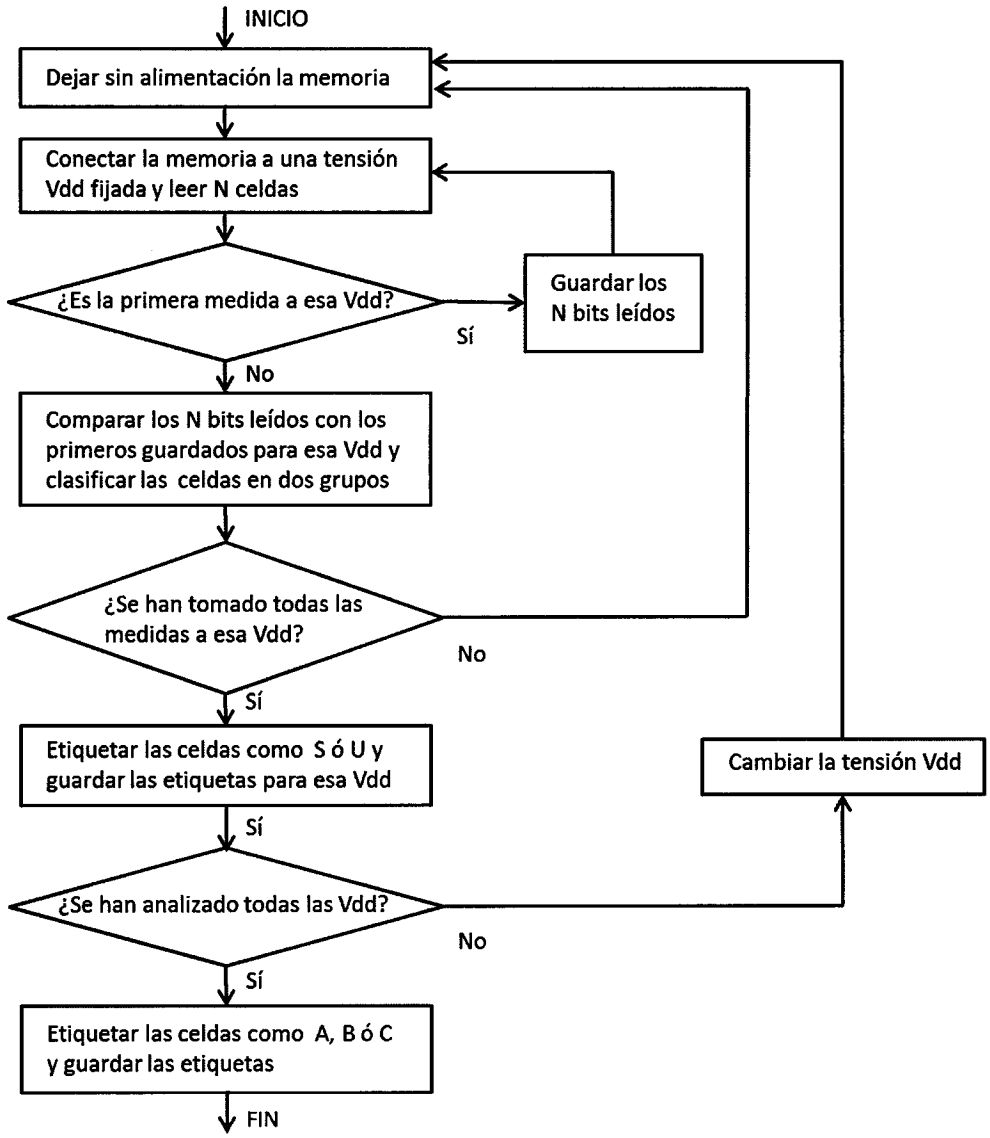

INICIO
Dejar sin alimentación la memoria
Conectar la memoria a una tensión Vdd fijada y leer N celdas
¿Es la primera medida a esa Vdd?
Sí
Guardar los N bits leídos
No
Comparar los N bits leídos con los primeros guardados para esa Vdd y clasificar las celdas en dos grupos
¿Se han tomado todas las medidas a esa Vdd?
No
Sí
Etiquetar las celdas como S ó U y guardar las etiquetas para esa Vdd
Cambiar la tensión Vdd
Sí
¿Se han analizado todas las Vdd?
No
Sí
Etiquetar las celdas como A, B ó C y guardar las etiquetas
FIN

Figura 1

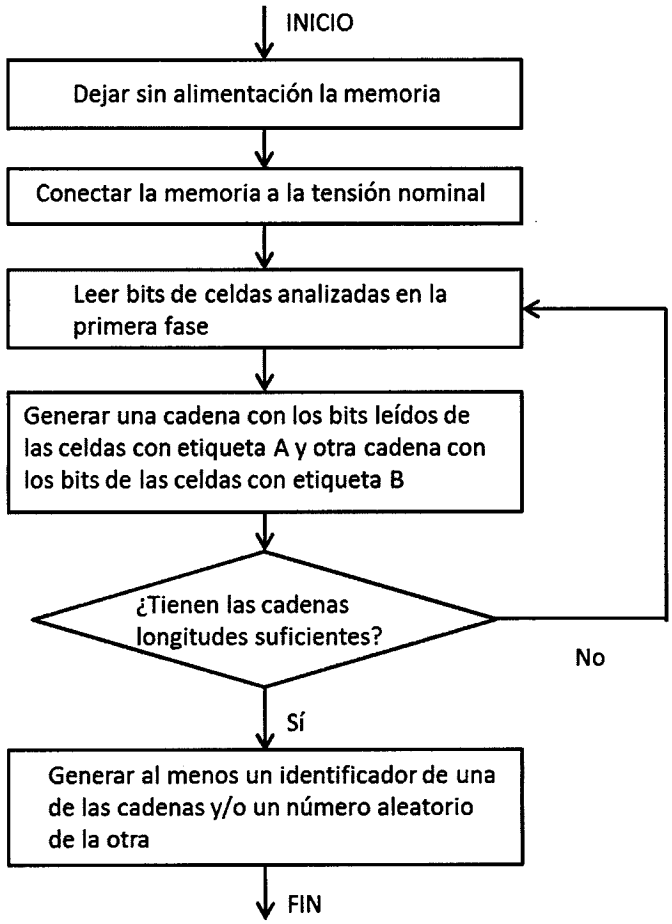

INICIO
Dejar sin alimentación la memoria
Conectar la memoria a la tensión nominal
Leer bits de celdas analizadas en la primera fase
Generar una cadena con los bits leídos de las celdas con etiqueta A y otra cadena con los bits de las celdas con etiqueta B
¿Tienen las cadenas longitudes suficientes?
No
Sí
Generar al menos un identificador de una de las cadenas y/o un número aleatorio de la otra
FIN

Figura 2

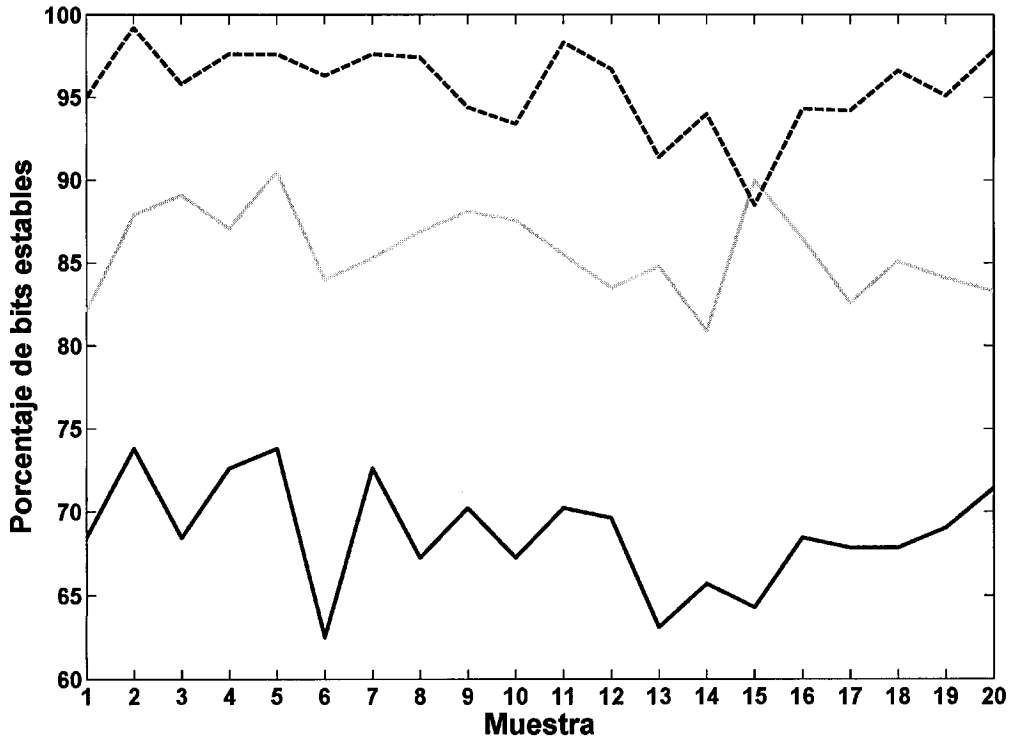


Figura 3

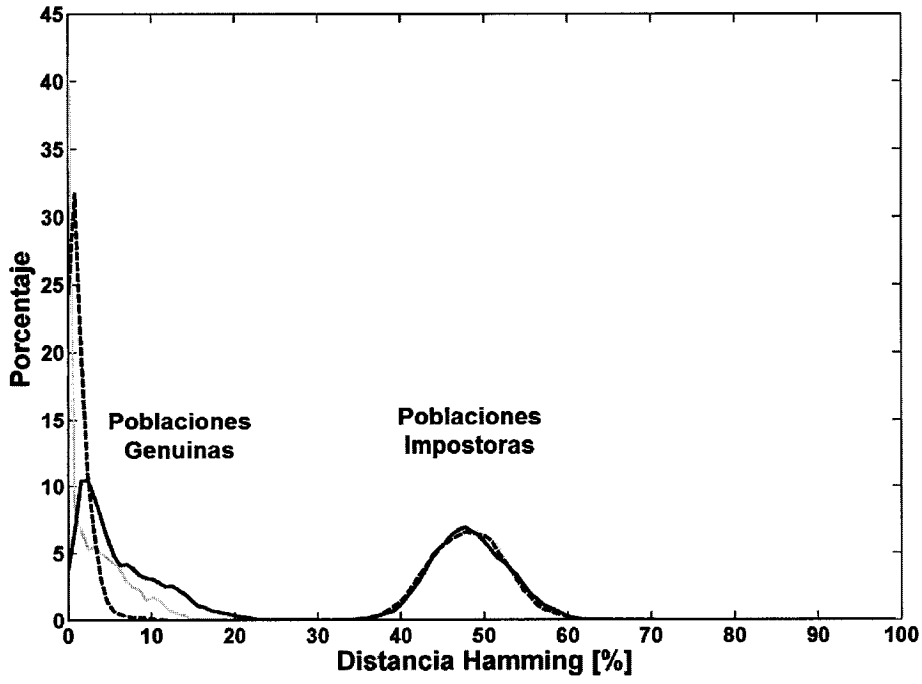
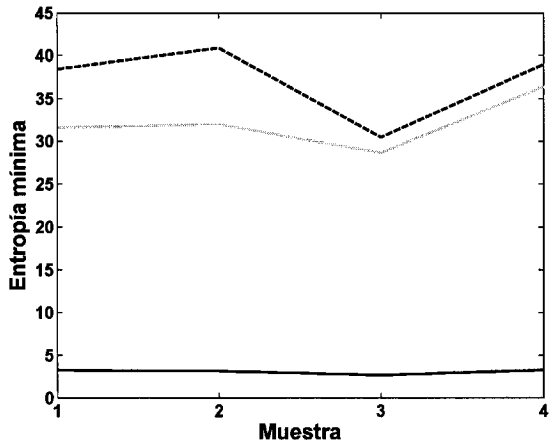
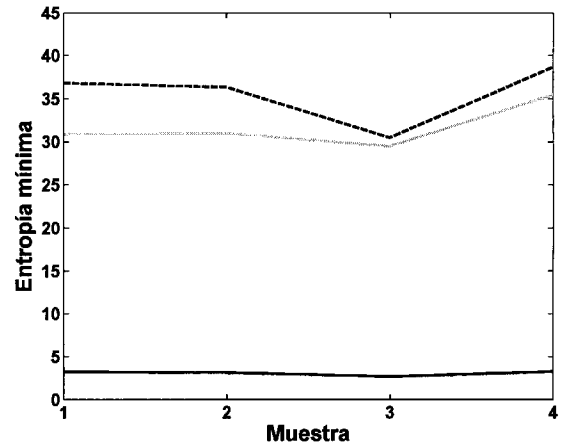


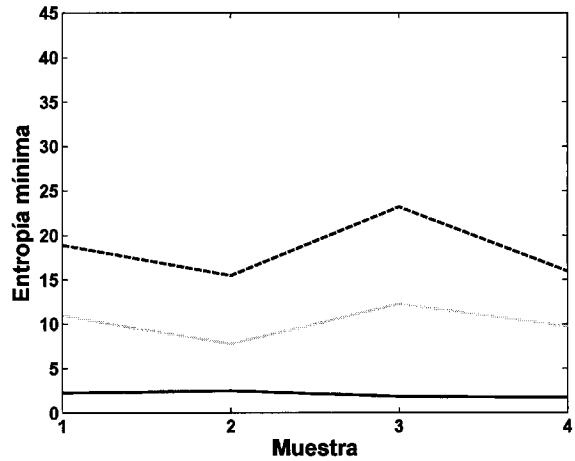
Figura 4


Entropía mínima
Muestra
0
5
10
15
20
25
30
35
40
45
1
2
3
4

(a)


Entropía mínima
Muestra
0
5
10
15
20
25
30
35
40
45
1
2
3
4

(b)


Entropía mínima
Muestra
0
5
10
15
20
25
30
35
40
45
1
2
3
4

(c)

Figura 5

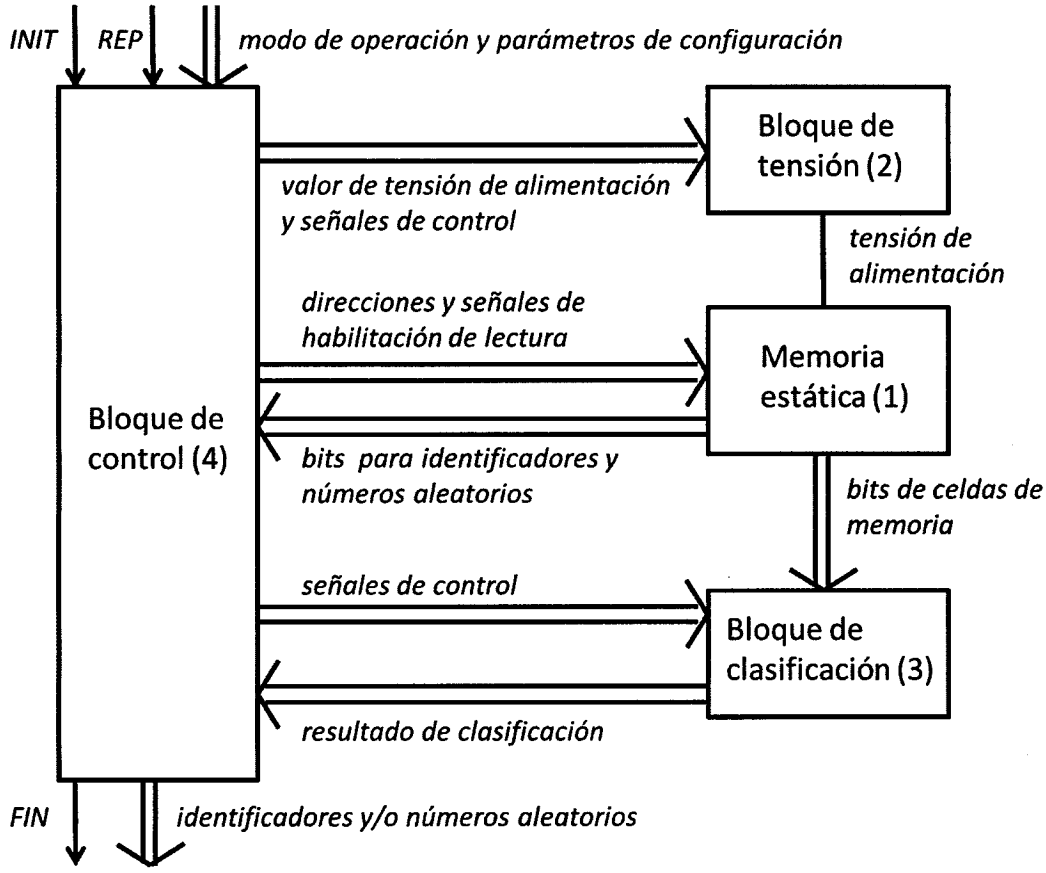

INIT
REP
modo de operación y parámetros de configuración
Bloque de tensión (2)
valor de tensión de alimentación y señales de control
tensión de alimentación
direcciones y señales de habilitación de lectura
Memoria estática (1)
Bloque de control (4)
bits para identificadores y números aleatorios
bits de celdas de memoria
señales de control
Bloque de clasificación (3)
resultado de clasificación
FIN
identificadores y/o números aleatorios

Figura 6

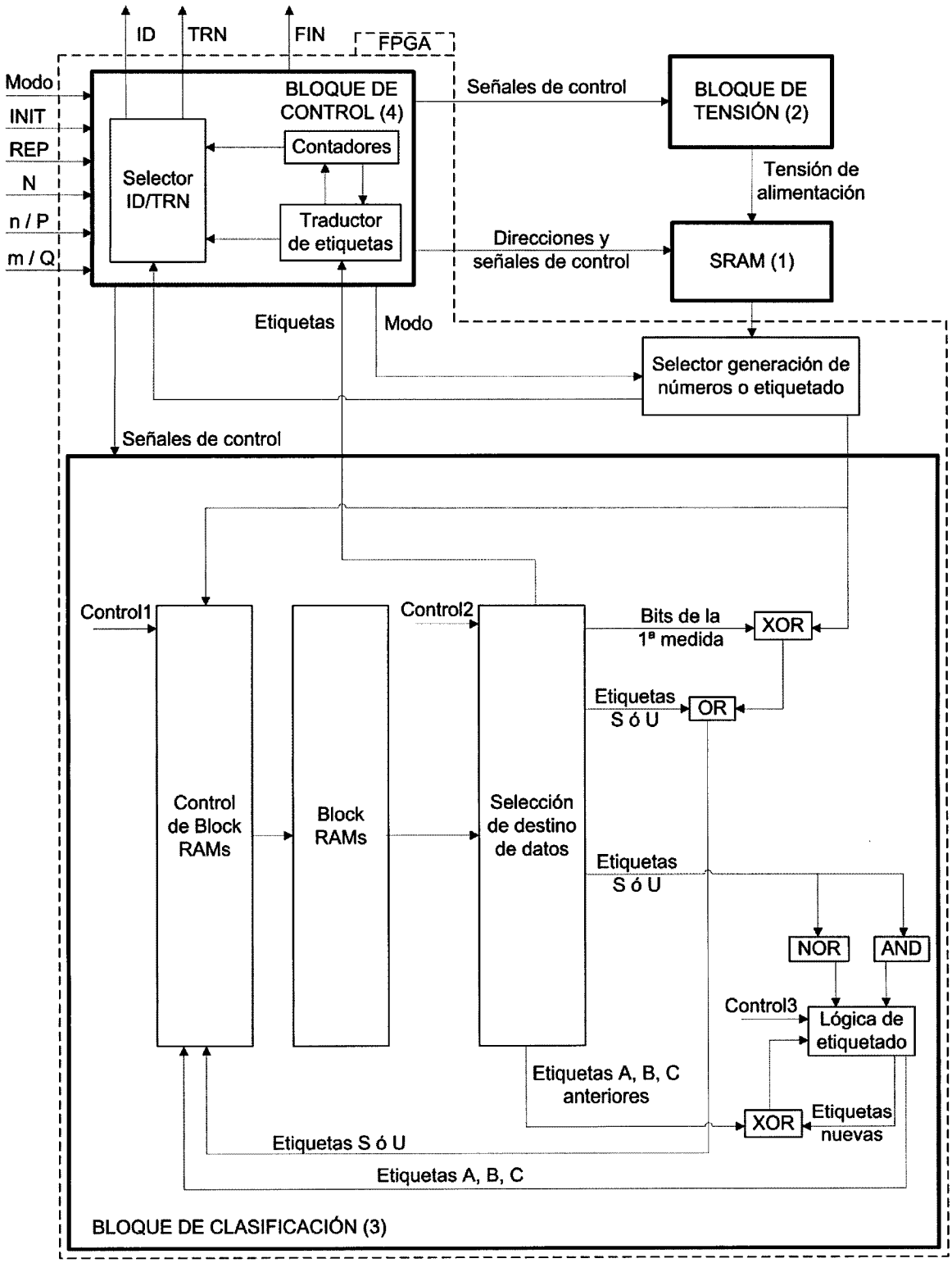

ID
TRN
FIN
FPGA
Modo
INIT
REP
N
n / P
m / Q
BLOQUE DE CONTROL (4)
Selector ID/TRN
Contadores
Traductor de etiquetas
Señales de control
BLOQUE DE TENSIÓN (2)
Tensión de alimentación
Direcciones y señales de control
SRAM (1)
Etiquetas
Modo
Selector generación de números o etiquetado
Señales de control
Control1
Control2
Bits de la 1ª medida
XOR
Etiquetas S ó U
OR
Control de Block RAMs
Block RAMs
Selección de destino de datos
Etiquetas S ó U
NOR
AND
Control3
Lógica de etiquetado
Etiquetas A, B, C anteriores
XOR
Etiquetas nuevas
Etiquetas S ó U
Etiquetas A, B, C
BLOQUE DE CLASIFICACIÓN (3)

Figura 7