

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

Señor(a)
UNIVERSIDAD INDUSTRIAL DE SANTANDER

TÍTULO DE LA SOLICITUD: “FUENTES DE CADENA ALEATORIA DE BITS USANDO FUENTES DÉBILES”

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486.

Por lo tanto, se estudiarán las reivindicaciones 1 a 16 del radicado N° NC2017/0008879 del 30 de agosto de 2017.

El problema planteado en esta solicitud consiste en la necesidad de suministrar un generador de números aleatorios con distribución cercana a la uniforme que parta de dos fuentes de entropías con algún tipo de sesgo y obtenga una fuente de alta aleatoriedad y de alta resistencia a ataques.

Para resolver este problema técnico, la solicitud en estudio proporciona un generador de números aleatorios que comprende: una unidad determinística de muestreo con una primera entrada, una segunda entrada y una salida, una primera fuente de entropía conectada a la primera entrada de la unidad determinística de muestreo, una segunda fuente de entropía conectada a la segunda entrada de la unidad determinística de muestreo, una unidad determinística de posprocesamiento conectada a la salida de la unidad determinística de muestreo (Resumen).

2. De la solicitud de patente

2.1. Título

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

El solicitante en el escrito radicado bajo el N° NC2017/0008879 del 30 de agosto de 2017, tituló la invención como: “FUENTES DE CADENA ALEATORIA DE BITS USANDO FUENTES DÉBILES”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente:



Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

“DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA”.

2.2. Reivindicaciones (Art. 30 Decisión 486)

- La frase “una *unidad determinística de muestreo*”, presente en la reivindicación 1 sugiere un modelo matemático, lo cual no corresponde a materia patentable, por lo tanto se sugiere eliminar el término “determinística” y describir las unidades y las fuentes de entropía en términos del hardware con el cual se logra la generación de números aleatorios.
- Las reivindicaciones 5, 7 y 13 describen los mismos elementos, por lo tanto, repiten la misma materia. Se sugiere eliminar las cláusulas que contienen materia repetida.

3. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 30 de agosto de 2017 que corresponde a la fecha de presentación nacional.

Consultadas las fuentes de información con que se cuenta, se encontró el siguiente documento que anticipa el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US20160204781	“Systems and methods for leveraging path delay variations in a circuit and generating error-tolerant bitstrings”	14 de Julio de 2016

El documento D1¹ divulga un PUF de retardo incorporado en el hardware (HELP) que aprovecha la entropía al monitorear la estabilidad de la ruta y medir los retrasos de la ruta desde las macros lógicas centrales. HELP incorpora técnicas para lidiar con el sesgo. Una característica única de HELP es que puede comparar datos medidos de diferentes estructuras de prueba. HELP puede implementarse en plataformas FPGA existentes. HELP puede aprovechar tanto la estabilidad del camino como las variaciones dentro del dado como fuentes de entropía (Resumen).

4. Examen de Patentabilidad (Art. 14 Decisión 486)

4.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “*un generador de números aleatorios que comprende: (...)*” (Radicado N° NC2017/0008879 del 30 de agosto de 2017).

Tabla 1. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1
Un generador de números aleatorios que comprende:	Esta divulgación se refiere a sistemas y métodos para generar cadenas de bits aleatorias y, más particularmente, a funciones físicamente no clonables (PUF) (Párr. 002).

¹<https://patentimages.storage.googleapis.com/db/61/84/6813caad7dcfc6/US20160204781A1.pdf>



Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

Una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y una salida.	Refiriéndose nuevamente a la FIG. 1, el controlador LC LFSR (1104) puede ser un registro de desplazamiento de retroalimentación lineal de 32 bits (LFSR) utilizado para producir los vectores de lanzamiento aleatorio. El Controlador REBEL (1106) puede configurar la IP en la fila REBEL asociada a la salida del bloque lógico AES. El motor de análisis de muestras (SAE) (1108) puede analizar los resultados digitalizados en la cadena de retardo después de cada prueba de LC para una ruta determinada y determina si la ruta es "válida". Una ruta válida se define como una que tiene una transición real, es un error gratis, y produce resultados consistentes en múltiples muestras (...) (Párr. 0072). (...) El componente de desafío para HELP PUF (1000) puede incluir una secuencia de prueba de dos vectores seleccionada al azar aplicada a las entradas de la macro-prueba (MUT) La secuencia de prueba puede introducir un conjunto de transiciones que se propagan a través de la lógica central del MUT y aparecen en sus salidas (...) (Párr. 0061).
Una primera fuente de entropía (1a) conectada a la primera entrada de la unidad determinística de muestreo (3).	(...) Aunque no es deseable desde una perspectiva de diseño, las variaciones eléctricas introducidas por las variaciones del proceso definen la fuente de entropía en la que se basan los PUF (...) (Párr. 0048). Un PUF de retardo incorporado en el hardware (HELP) aprovecha la entropía al monitorear la estabilidad de la ruta y medir los retrasos de la ruta desde las macros lógicas centrales. HELP incorpora técnicas para lidiar con el sesgo. Una característica única de HELP es que puede comparar datos medidos de diferentes estructuras de prueba. HELP puede implementarse en plataformas FPGA² existentes. HELP puede aprovechar tanto la estabilidad del camino como las variaciones dentro del dado como Fuentes de entropía (Resumen).
Una segunda fuente de entropía (2a) conectada a la segunda entrada de la unidad de muestreo (3).	(...) Las fuentes de entropía propuestas incluyen variaciones en los voltajes de umbral del transistor, en los retrasos de propagación en las cadenas del inversor y los RO, en los patrones de encendido en las SRAM, en la corriente de fuga, en la resistencia del metal y muchos otros (...) (Párr. 0050). Un PUF de retardo incorporado en el hardware (HELP) aprovecha la entropía al monitorear la estabilidad de la ruta y medir los retrasos de la ruta desde las macros lógicas centrales. HELP incorpora técnicas para lidiar con el sesgo. Una característica única de HELP es que puede comparar datos medidos de diferentes estructuras de prueba. HELP puede implementarse en plataformas FPGA³ existentes. HELP puede aprovechar tanto la estabilidad del camino como las variaciones dentro del dado como Fuentes de entropía (Resumen).
Una unidad determinística de posprocesamiento (4) conectada a la salida de la unidad determinística de muestreo (3).	La mayoría de los PUF están diseñados utilizando primitivas de circuito idénticas como un medio para evitar sesgos. Este no es el caso de HELP (1100), porque los PUT varían ampliamente en longitud. En este documento se describe una técnica desarrollada llamada "Recuento de PN dual" (DPNC) que procesa posteriormente las PN para eliminar este sesgo. La

² https://en.wikipedia.org/wiki/Field-programmable_gate_array
³ https://en.wikipedia.org/wiki/Field-programmable_gate_array

Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

0 o 1. Las secuencias de bits de respuesta producidas por una secuencia de desafíos definen la cadena de bits (Párr. 0150).

La figura 2 es un diagrama de bloques que ilustra un ejemplo de una estructura de prueba integrada que puede implementar uno o más técnicas de esta divulgación (Párr. 0014). En esta figura se muestran flip-flops⁵ que pueden ser construidos a partir de compuertas NAND o NOR (Pág. 3, Fig. 2).

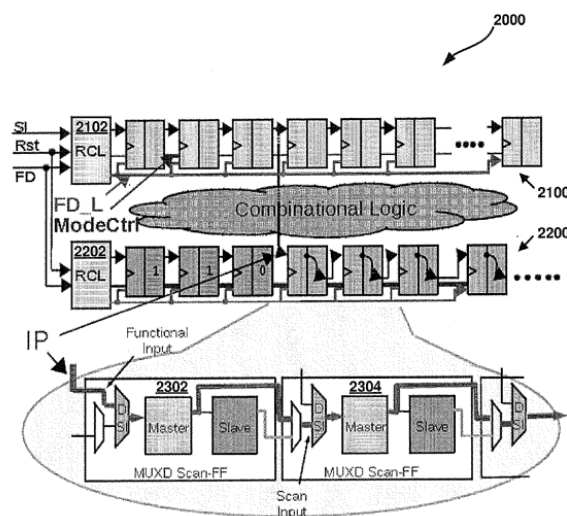


FIG. 2

- Reivindicación 3: Cabe señalar que la precisión de la medición del retraso afecta la estabilidad de HELP (1000). Se utilizó una estructura de prueba integrada llamada REBEL para obtener representaciones digitalizadas de alta precisión de los retrasos de la ruta. En un ejemplo, REBEL se integra directamente con la lógica de la cadena de escaneo y utiliza la red de árbol de reloj en chip para los eventos de temporización de captura de lanzamiento (LC). La figura 2 es un diagrama de bloques que ilustra un ejemplo de una estructura de prueba integrada que puede implementar una o más técnicas de esta divulgación. La fig. 2 representa una visión general de una estructura de prueba REBEL. Como se ilustra en la FIG. 2, la estructura de prueba REBEL (2000) incluye dos filas de flip-flops (FF), (2100 y 2200) conectadas entre sí en una cadena de escaneo. Los pequeños bloques lógicos, (2102 y 2202), a la izquierda de cada fila, etiquetados como RCL para Row Control Logic, permiten que los elementos de escaneo en cada fila se configuren de la siguiente manera: La fila superior (2100) es la fila de inicio y está configurada para funcionar en modo funcional modo. La segunda fila (2200) es la fila de captura, y se configura en "modo mixto", en el que se elige un FF específico, llamado punto de inserción (IP). Este scan-FF y cada scan-FF a su derecha en la fila se colocan en modo de "retardo de descarga" (descrito a continuación), y forman una cadena de retardo combinacional, extendiendo efectivamente la ruta en la IP (Párr. 0062) (...) Aunque no es deseable desde una perspectiva de diseño,

⁵ [https://en.wikipedia.org/wiki/Flip-flop_\(electronics\)](https://en.wikipedia.org/wiki/Flip-flop_(electronics))



Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

las variaciones eléctricas introducidas por las variaciones del proceso definen la fuente de entropía en la que se basan los PUF (...) (Párr. 0048).

- Reivindicaciones 5, 7 y 13: La principal característica distintiva de los sistemas PUF es la fuente de entropía que aprovechan. Las fuentes de entropía propuestas incluyen variaciones en los voltajes de umbral del transistor, en los retrasos de propagación en las cadenas del inversor y los RO, en los patrones de encendido en las SRAM, en la corriente de fuga, en la resistencia del metal y muchos otros. Las PUF miden y digitalizan las variaciones naturales que se producen en los retrasos de ruta, la corriente de fuga, los patrones de encendido de SRAM, etc. para producir una secuencia larga de bits aleatorios, es decir, una cadena de bits. Los diseños de PUF propuestos generalmente se dividen en una de las siguientes clasificaciones: PUF de SRAM, osciladores de anillo, PUF de corriente de impulsión MOS, PUF de línea de retardo y árbitro y PUF basados en variaciones en los cables de metal de un chip. Los PUF basados en demoras también incluyen diseños como el Glitch PUF, que aprovecha la variación en el comportamiento de falla. Cada uno de estos PUF aprovecha una o más propiedades que varían naturalmente, y casi todos los PUF comparten un conjunto común de desafíos, tales como error de medición e incertidumbre, y fluctuaciones en el voltaje o la temperatura (...) (Párr. 0050).
- Reivindicación 8: Como se mencionó anteriormente, la fuente de entropía para HELP se define a partir de dos componentes; estabilidad del camino y variaciones dentro del dado en el retraso. Esta doble fuente de entropía es un beneficio significativo para mejorar la aleatoriedad de las cadenas de bits generadas, así como para aumentar la dificultad de los ataques de ingeniería inversa. En una implementación FPGA del Estándar de cifrado avanzado (AES) como macro central, se descubrió que ambas fuentes de entropía proporcionaban un alto grado de aleatoriedad en las cadenas de bits generadas. Se pueden usar varios métodos de generación de cadenas de bits con la implementación de FPGA del AES, incluido uno de los cuales aprovecha solo la fuente de entropía de estabilidad de ruta, a la que aquí se hace referencia como Universal, Sin Módulo o UNM (Párr. 0122). Las figuras 28A y FIG. 28B son diagramas esquemáticos de circuitos TDC que pueden implementar una o más técnicas de esta descripción. Como se ilustra en la FIG. 28A y FIG. 28B, TDC 28000 se muestra como recibiendo puntos de derivación ARB como entrada y TDC 29000 se muestra como recibiendo una entrada de una fuente de entropía más general 29002. En aras de la brevedad, el funcionamiento de TDC 28000 y TDC 29000 se describirá colectivamente con respecto a la figura 28A (Párr. 0155) (Pág. 29, Fig. 28A). En la figura 28A se aprecia (azul y rojo) que los elementos generadores que constituyen el dispositivo elementos de hardware y que se pueden montar en un FPGA pueden intercambiarse (Pág. 29, Fig. 28A).



Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

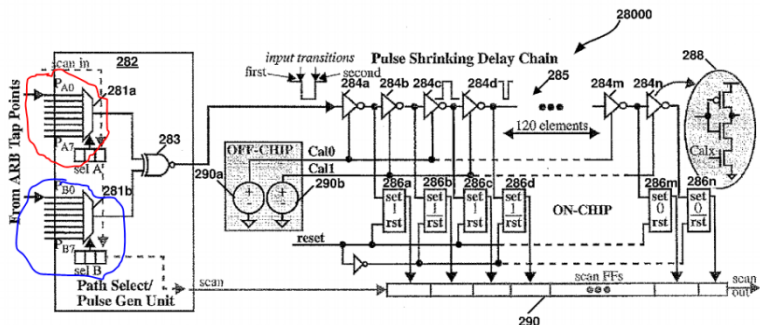


FIG. 28A

Las reivindicaciones dependientes a 3, 5, 7, 8 y 13 tampoco cumplen con el requisito de novedad.

5. Conclusión con respecto a novedad y/o nivel inventivo

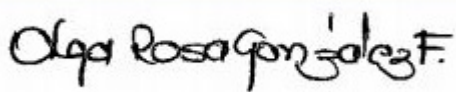
Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20160204781	1 a 3, 5, 7, 8 y 13	Novedad

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presenta un nuevo capítulo reivindicatorio deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única y la Dirección de Nuevas Creaciones seguirá el procedimiento descrito en el numeral 1.2.2.5.1.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



OLGA ROSA GONZÁLEZ FONSECA
DIRECTORA DE NUEVAS CREACIONES (E)

Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

**INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD**

Solicitud No.		Examen de patentabilidad							
NC2017/0008879		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
30/08/2017						X			
Solicitante									
UNIVERSIDAD INDUSTRIAL DE SANTANDER									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 16					
Palabras clave utilizadas				PBRs, Random Generator, Bits, Entropy, gates, flip- flop.					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 7/58				
DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)									
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP(1)	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica			Categoría del documento citado(2)		
SIPI	14099010	08/05/2014	-	-			A		
PATBASE	US20160204781	14/07/2016	1 a 3, 5, 7, 8 y 13	Todo el Documento			X		
	US2014122552	01/09/2015	-	-			A		
	US2014254640	11/09/2014	-	-			A		
	US2014003805	26/05/2015	-	-			A		
(1) Cita completa literatura no patente (LNP)									
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.									
O									
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.									
(2) Categorías de documentos citados									
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante.									
“E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.									
“L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de									
“T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos.									

Oficio N° 2271 de 13 de febrero de 2020

Ref. Expediente N° NC2017/0008879

prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.	“X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: (10/02/2020)	
Examinador: JUAN SEBASTIAN RONCANCIO AREVALO	