REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

Señor(a)
UNIVERSIDAD INDUSTRIAL DE SANTANDER

TÍTULO DE LA SOLICITUD: ***"DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA"***

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. Modificaciones presentadas (Art. 34 Decisión 486)

Se aceptan las modificaciones radicadas el 12 de mayo de 2020, bajo el número NC2017/0008879, por ajustarse a los requisitos legales.

2. 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 14 del radicado N° NC2017/0008879 del 12 de mayo de 2020.

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).

3. De la solicitud de patente

3.1. 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.

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

De acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2017/0008879 del 12 de mayo de 2020 y teniendo en cuenta el objeto de la solicitud, se acepta el título siguiente: “DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA”.

4. 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
D2	US2017090872	“Random Number Generator”	30 de marzo de 2017
D3	US2008022039	“Random number generation”	24 de enero de 2008

El documento D2[1] divulga un procesador incluye una unidad de ejecución para generar un número aleatorio. La unidad de ejecución incluye circuitos de fuente de entropía, circuitos de correlación y un circuito extractor. Los circuitos fuente de entropía incluyen componentes totalmente digitales y deben generar un flujo de bits aleatorio inicial. Los circuitos de correlación son para eliminar correlaciones del flujo de bits aleatorio inicial para producir un flujo de bits aleatorio intermedio. El circuito extractor debe seleccionar un subconjunto del flujo de bits aleatorio intermedio como una salida aleatoria de la unidad de ejecución (Resumen).

El documento D3[2] divulga un controlador para controlar el funcionamiento de una unidad de disco duro que es capaz de generar un número aleatorio utilizando la unidad de disco duro. Inicialmente, la unidad de disco duro no puede realizar una operación de lectura anticipada. Las direcciones aleatorias en el disco duro se generan a partir de la salida del generador de números pseudoaleatorios. Los comandos de verificación de lectura se envían al disco duro para realizar una operación de verificación de lectura de lectura y verificación de los datos almacenados en los sectores del disco duro en las direcciones aleatorias sin devolver los datos. Se miden los tiempos de acceso al disco que tarda la unidad de disco duro para acceder a los sectores. Se realiza un proceso de alineación en un número plural de mediciones de tiempo de acceso al disco para generar un número aleatorio (Resumen).

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

5.1. Nivel inventivo (Art 18 Decisión 486)

La reivindicación 1 consiste en: *“Un generador de números aleatorios que comprende (…)”* (Radicado No. NC2017/0008879 del 12 de mayo de 2020).

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

Características esenciales	D2	D3
Un generador de números aleatorios que comprende.	Generador de números aleatorios (Título).	Generación de números aleatorios (Título).
Una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y	Como se discutió anteriormente, RNG (1828) puede utilizar una o más fuentes de entropía totalmente	Los números aleatorios generados por el controlador (10) pueden ser utilizados por el aparato informático

[1] https://patentimages.storage.googleapis.com/fe/35/01/51eb0428002ad0/US20170090872A1.pdf
[2] https://patentimages.storage.googleapis.com/b5/d3/7a/7d7af2ea46a0d2/US20080022039A1.pdf

una salida, donde la unidad determinística de muestreo (3) está configurada para generar a partir de una semilla un número compuesto de números con distribución estadística cercana a la uniforme.	digitales. Estas fuentes se pueden utilizar en lugar de una variedad de fuentes que utilizan fenómenos físicos no deterministas, como la fluctuación de fase, la descomposición suave de óxido y el ruido térmico. Los flujos de bits sin procesar producidos por generadores de números aleatorios basados en ruido térmico pueden mostrar altos niveles de entropía y pueden cumplir con los estándares de la industria. Sin embargo, la presente descripción reconoce que estos todavía pueden contener no uniformidades y correlaciones en serie debido a variaciones de proceso aleatorias de 6σ, ruido intermitente de suministro/acoplamiento de alta frecuencia y artefactos de bucle de control de retroalimentación. La presente descripción reconoce que estas condiciones pueden hacer que tales fuentes de entropía sean subóptimas en, por ejemplo, el uso directo como generadores de claves criptográficas de entropía completa en entornos de fabricación de alto volumen. Si bien algunos generadores de números aleatorios pueden superar las no idealidades en fuentes analógicas mediante el uso de funciones clave para procesar posteriormente la salida de una sola fuente de entropía no uniforme, la presente divulgación reconoce que estos pueden requerir un área significativa en un dado, como más de 30,000 puertas. Además, pueden requerir altas cantidades de energía. En consecuencia, RNG (1828) puede ser preferible para su uso en aplicaciones de plataforma de bajo consumo de energía, Internet de las cosas (IoT) y usable (Párr. 0088). El supresor de correlación (2400) puede constituir un circuito de acondicionamiento que transforma la aleatoriedad no uniforme de los flujos de bits sin procesar en una distribución uniforme criptográficamente útil (…) (Párr. 0110). No menciona que la generación de números aleatorios se haga a partir de una semilla.	(20) en una serie de aplicaciones diferentes. La aplicación destinada principalmente es una aplicación criptográfica. En este caso, el número aleatorio generado por el controlador (10) puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios. Opcionalmente, dicho generador de números pseudoaleatorios puede incorporarse en el controlador (10) u otro componente del aparato informático (20). Sin embargo, el número aleatorio generado puede aplicarse igualmente a otras aplicaciones en el aparato informático (20) que requieren un número aleatorio (Párr. 0093). Los números aleatorios juegan un papel importante en las aplicaciones criptográficas seguras. El núcleo de todas las aplicaciones criptográficas es la generación de un número aleatorio que no se conoce y que un adversario no puede cuestionar. El número aleatorio debe ser adecuadamente aleatorio para que un adversario tenga una baja probabilidad de violar el sistema criptográfico en un tiempo razonable mediante una técnica sistemática de prueba y error. En términos generales, las propiedades requeridas del número aleatorio generado es que la distribución de los números generados es uniforme, sin distorsiones, consistente, impredecible, escalable e independiente (Párr. 0004).
Una primera fuente de entropía (1a) conectada a la primera entrada de la unidad determinística de muestreo (3). Una segunda fuente de entropía (2a) independiente de la primera fuente de entropía (1a) y	En una realización, RNG (1828) puede combinar la entropía de una o más fuentes de entropía independientes para generar un número aleatorio. Por ejemplo, RNG (1828) puede combinar tres de esas fuentes. En una realización	Si bien la generación de números aleatorios descrita anteriormente utiliza mediciones del tiempo de acceso al disco del disco duro (1) como la única fuente de entropía en la generación de un número aleatorio, se apreciará que el

conectada a la segunda entrada de la unidad determinística de muestreo (3), donde la segunda fuente de entropía (2a) está configurada para proporcionar la semilla a la unidad determinística de muestreo (3).	adicional, RNG (1828) puede utilizar una o más fuentes de entropía totalmente digitales para generar un número aleatorio. En otra realización adicional, RNG (1828) puede utilizar uno o más recursos de entropía autocalibrados para generar un número aleatorio. En otra realización más, RNG (1828) puede incluir circuitos extractores para generar un flujo de bits de salida a partir de sus fuentes de entropía. En otra realización más, RNG (1828) puede incluir un extractor ligero. El extractor ligero puede incluir un extractor Barack-Impagliazzo-Widgersen (BIW) de un tamaño de 8 bits. El extractor puede realizarse en aproximadamente 1.3K puertas (Párr. 0082). No se menciona la etapa de proporcionar la semilla.	número aleatorio podría generarse adicionalmente utilizando una fuente de entropía adicional disponible en el aparato informático (20). En este caso, las mediciones del tiempo de acceso al disco se pueden mezclar con las mediciones derivadas de la otra fuente de entropía. Tal mezcla de mediciones de diferentes fuentes de entropía es en sí conocida (Párr. 0091). La fuente de entropía es una fuente de números variables, que pueden ser bits individuales, derivados de la medición de un fenómeno físico que tiene cierto grado de aleatoriedad. En general, la salida de números variables de cualquier fuente de entropía dada puede estar sesgada o sesgada en cierta medida (por lo que la distribución no es uniforme) y/o correlacionada (por lo que los números sucesivos dependen unos de otros). Se ha propuesto una gran cantidad de fuentes de entropía para su uso en la generación de números aleatorios en un aparato informático. Algunos ejemplos de tales fuentes de entropía conocidas son (…) (Párr. 0006). Los números aleatorios generados por el controlador (10) pueden ser utilizados por el aparato informático (20) en una serie de aplicaciones diferentes. La aplicación destinada principalmente es una aplicación criptográfica. En este caso, el número aleatorio generado por el controlador (10) puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios. Opcionalmente, dicho generador de números pseudoaleatorios puede incorporarse en el controlador (10) u otro componente del aparato informático (20). Sin embargo, el número aleatorio generado puede aplicarse igualmente a otras aplicaciones en el aparato informático (20) que requieren un número aleatorio (Párr. 0093). No menciona que se la unidad de muestreo sea determinista.
Una unidad determinística de posprocesamiento (4) conectada a la salida de la unidad determinística de muestreo (3), donde la unidad determinística de posprocesamiento (4) está configurada para reducir el sesgo del número generado en la unidad determinística de muestreo (3) posprocesándolo para generar un	Sin embargo, las variaciones de temperatura del voltaje del proceso, los desajustes inducidos por el envejecimiento o el ruido acoplado pueden alterar este comportamiento ideal al introducir sesgos que favorecen la resolución hacia un estado (cero o uno). En una realización, la fuente (2100) puede incluir el ajuste de los	Para lidiar con esto, se realiza un proceso de alineación en la salida de la fuente de entropía. El proceso de compensación reduce el sesgo y la correlación en la salida de la fuente de entropía. Idealmente, el proceso de alineación produce una distribución de probabilidad uniforme sin correlación. Se conoce una gran cantidad de procesos de alineación,

dato de salida.	inversores (2110, 2112) para superar los sesgos. Por ejemplo, los inversores (2110) pueden implementarse con múltiples transistores NMOS y PMOS. En una realización adicional, la fuente (2100) puede aplicar bits de configuración a los inversores (2110, 2112), que pueden usar los bits de configuración para sesgar las patas del transistor para modular las intensidades relativas de los transistores, afectando así la salida. Por ejemplo, los bits para ajustar las patas del transistor NMOS se pueden denotar como "nconf" y los bits para ajustar las patas del transistor PMOS se pueden denotar como "pconf". El número de bits puede depender de la implementación particular en los inversores (2110, 2112). Por ejemplo, se pueden usar cinco bits para nconf y dos bits para pconf. Un nconf y pconf pueden estar disponibles individualmente para cada uno de los inversores (2110, 2112). Los bits pueden especificar si las patas paralelas NMOS o PMOS dadas deben activarse o desactivarse. El resultado puede ser una modulación de las intensidades del transistor, que tiende a sesgar la salida a cero o a uno. La sintonización de los inversores (2110, 2112) puede ser gruesa en comparación con la sintonización de otros elementos, como los retrasos sintonizables (2104, 2106) (Párr. 0101).	algunos ejemplos son los siguientes: calcular la paridad usando una función OR exclusiva; aplicar un mapeo de transición tal como un mapeo de von Neumann; realizar una transformación de frecuencia, por ejemplo, una Transformada rápida de Fourier; y aplicando una técnica de compresión reversible (Párr. 0012).

El documento D2 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque divulga un generador de números aleatorios (Título).

La diferencia entre la invención definida en la reivindicación 1 y el dispositivo divulgado de D2 consiste en que la solicitud en estudio incluye que la unidad determinística de muestreo está configurada para generar un número a partir de una semilla.

El efecto que se logra al incluir que la unidad determinística de muestreo está configurada para generar un número a partir de una semilla es generar un número aleatorio que luego es posprocesado por la unidad determinística de posprocesamiento para generar el dato de salida.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el dispositivo conocido en D2 con el fin de generar un número aleatorio que luego es posprocesado por la unidad determinística de posprocesamiento para generar el dato de salida?

Sin embargo, el incluir que la unidad determinística de muestreo está configurada para generar un número aleatorio a partir de una semilla para generar un número que luego es posprocesado por la unidad determinística de posprocesamiento para generar el

dato de salida, ya está divulgado en el documento D3 en el siguiente aparte: Los números aleatorios generados por el controlador (10) pueden ser utilizados por el aparato informático (20) en una serie de aplicaciones diferentes. La aplicación destinada principalmente es una aplicación criptográfica. En este caso, el número aleatorio generado por el controlador (10) puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios. Opcionalmente, dicho generador de números pseudoaleatorios puede incorporarse en el controlador (10) u otro componente del aparato informático (20). Sin embargo, el número aleatorio generado puede aplicarse igualmente a otras aplicaciones en el aparato informático (20) que requieren un número aleatorio (Párr. 0093). Los números aleatorios juegan un papel importante en las aplicaciones criptográficas seguras. El núcleo de todas las aplicaciones criptográficas es la generación de un número aleatorio que no se conoce y que un adversario no puede cuestionar. El número aleatorio debe ser adecuadamente aleatorio para que un adversario tenga una baja probabilidad de violar el sistema criptográfico en un tiempo razonable mediante una técnica sistemática de prueba y error. En términos generales, las propiedades requeridas del número aleatorio generado es que la distribución de los números generados es uniforme, sin distorsiones, consistente, impredecible, escalable e independiente (Párr. 0004).

En consecuencia, la persona normalmente versada en la materia al verse enfrentada al problema técnico objetivo de generar un número aleatorio que luego es posprocesado por la unidad determinística de posprocesamiento para generar el dato de salida, estaría motivada a incluir que la unidad determinística de muestreo está configurada para generar un número aleatorio a partir de una semilla del documento D3 en el dispositivo de D2, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Asimismo, el documento D3 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 6: Los números aleatorios generados por el controlador (10) pueden ser utilizados por el aparato informático (20) en una serie de aplicaciones diferentes. La aplicación destinada principalmente es una aplicación criptográfica. En este caso, el número aleatorio generado por el controlador (10) puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios. Opcionalmente, dicho generador de números pseudoaleatorios puede incorporarse en el controlador (10) u otro componente del aparato informático (20). Sin embargo, el número aleatorio generado puede aplicarse igualmente a otras aplicaciones en el aparato informático (20) que requieren un número aleatorio (Párr. 0093).

La reivindicación dependiente 6 no menciona alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al dispositivo de la reivindicación 1, por lo cual se considera que no tiene nivel inventivo.

6. 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
D2	US2017090872	1	Nivel Inventivo
D3	US2008022039	1 y 6	Nivel Inventivo

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

7. Respuesta a los argumentos del solicitante

El solicitante indica que: "*D1 no divulga dos fuentes de entropía*".

Con respecto a lo anterior se le indica al señor que si bien el documento D1 no divulga dos fuentes de entropía, se ha realizado una nueva búsqueda encontrando el nuevo documentos D2 que recita: En una realización, RNG (1828) puede combinar la entropía de una o más fuentes de entropía independientes para generar un número aleatorio. Por ejemplo, RNG (1828) puede combinar tres de esas fuentes. En una realización adicional, RNG (1828) puede utilizar una o más fuentes de entropía totalmente digitales para generar un número aleatorio. En otra realización adicional, RNG (1828) puede utilizar uno o más recursos de entropía auto calibrados para generar un número aleatorio. En otra realización más, RNG (1828) puede incluir circuitos extractores para generar un flujo de bits de salida a partir de sus fuentes de entropía. En otra realización más, RNG (1828) puede incluir un extractor ligero. El extractor ligero puede incluir un extractor Barack-Impagliazzo-Widgersen (BIW) de un tamaño de 8 bits. El extractor puede realizarse en aproximadamente 1.3K puertas (Párr. 0082)". Así mismo, el documento D3 recita: "Si bien la generación de números aleatorios descrita anteriormente utiliza mediciones del tiempo de acceso al disco del disco duro (1) como la única fuente de entropía en la generación de un número aleatorio, se apreciará que el número aleatorio podría generarse adicionalmente utilizando una fuente de entropía adicional disponible en el aparato informático (20). En este caso, las mediciones del tiempo de acceso al disco se pueden mezclar con las mediciones derivadas de la otra fuente de entropía. Tal mezcla de mediciones de diferentes fuentes de entropía es en sí conocida (Párr. 0091). La fuente de entropía es una fuente de números variables, que pueden ser bits individuales, derivados de la medición de un fenómeno físico que tiene cierto grado de aleatoriedad. En general, la salida de números variables de cualquier fuente de entropía dada puede estar sesgada o sesgada en cierta medida (por lo que la distribución no es uniforme) y/o correlacionada (por lo que los números sucesivos dependen unos de otros). Se ha propuesto una gran cantidad de fuentes de entropía para su uso en la generación de números aleatorios en un aparato informático. Algunos ejemplos de tales fuentes de entropía conocidas son (…) (Párr. 0006)". Tanto en el documento D2 como en el documento D3, se muestra que contienen dos fuentes de entropía. Dado lo anterior la solicitud en estudio no cumple con el requisito de Nivel inventivo a la luz de lo divulgado en los documentos D2 y D3 como se muestra en el presente oficio.

El solicitante indica que: "*D1 no divulga una primera fuente de entropía (1a) conectada a la primera entrada de una unidad determinística de muestreo (3);* ***y una segunda fuente de entropía (2a)*** ***independiente de la primera fuente de entropía (1a)*** *y conectada a la segunda entrada de la unidad determinística de muestreo (3);* ***donde la segunda fuente de entropía (2a) está configurada para proporcionar la semilla a la unidad de muestreo (3)"***.

Con respecto a lo anterior, se le indica al señor solicitante que si bien tanto D2 como D3 mencionan diferentes fuentes de entropía como se muestra en el párrafo anterior, específicamente con respecto al hecho de que una fuente produce la semilla de la otra fuente, D3 menciona: "Los números aleatorios generados por el controlador (10) pueden ser utilizados por el aparato informático (20) en una serie de aplicaciones diferentes. La aplicación destinada principalmente es una aplicación criptográfica. En este caso, el número aleatorio generado por el controlador (10) puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios. Opcionalmente, dicho generador de números pseudoaleatorios puede incorporarse en el controlador (10) u otro componente del

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

aparato informático (20). Sin embargo, el número aleatorio generado puede aplicarse igualmente a otras aplicaciones en el aparato informático (20) que requieren un número aleatorio (Párr. 0093)". En este caso el documento indica que el número aleatorio generado por el controlador puede usarse como semilla para un generador de números pseudoaleatorio para generar una secuencia más larga de números aleatorios, dado lo anterior, la solicitud en estudio no cumple con el requisito de Nivel inventivo a la luz de lo divulgado en los documentos D2 y D3 como se muestra en el presente oficio.

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.

Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES

Industria y Comercio
SUPERINTENDENCIA

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.	Examen de patentabilidad							
NC2017/0008879	1°		2°	X	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 14	
Palabras clave utilizadas	True, real, bit, generator, source, 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	US2017090872	30/03/2017	1	Todo el documento	Y
	US2008022039	24/01/2008	1 y 6	Todo el documento	Y
	WO17016609	02/02/2017	-		A
	US2013010952	10/01/2013	-	-	A
	TWI489376	21/06/2015	-	-	A
	US20160328211	10/11/2016	-	-	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://xxxxxxxx.

([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 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.

"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.

"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.

Industria y Comercio
SUPERINTENDENCIA

Oficio N° **12218** de **28 de septiembre de 2020**

Ref. Expediente N° NC2017/0008879

Fecha del reporte de búsqueda: (23/07/2020)
Examinador: JUAN SEBASTIAN RONCANCIO AREVALO