REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° **3548**

Ref. Expediente N° NC2017/0008879

Por la cual se otorga una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 26 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que mediante escrito radicado en esta Superintendencia el 30 de agosto de 2017 con el N° NC2017/0008879, por UNIVERSIDAD INDUSTRIAL DE SANTANDER, presentó la solicitud de patente de invención titulada "FUENTES DE CADENA ALEATORIA DE BITS USANDO FUENTES DÉBILES".

SEGUNDO: Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial Nº 854 el 8 de marzo de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

TERCERO: Que realizado el examen de fondo mediante Oficio N° 12218, notificado el 29 de septiembre de 2020, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

CUARTO: Que el solicitante mediante escrito radicado bajo el N° NC2017/0008879 el 9 de diciembre de 2020, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado Nº NC2017/0008879 el 12 de mayo de 2020.

QUINTO: Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *"Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial".*

SEXTO: Que en el presente caso las reivindicaciones 1 a 14 incluidas en el radicado bajo el N° NC2017/0008879 el 12 de mayo de 2020, cumplen los requisitos indicados en el considerando anterior, toda vez que refieren a un generador de números aleatorios, que difiere del estado de la técnica más cercano, US2017090872, en que la invención incluye una unidad determinística de muestreo con una primera entrada, una segunda entrada y una salida, donde la unidad determinística de muestreo está configurada para generar a partir de una semilla un número compuesto de números con distribución

estadística cercana a la uniforme, una segunda fuente de entropía independiente de la primera fuente de entropía y conectada a la segunda entrada de la unidad determinística de muestreo, donde la segunda fuente de entropía está configurada para proporcionar la semilla a la unidad determinística de muestreo, una unidad determinística de pos procesamiento conectada a la salida de la unidad determinística de muestreo, donde la unidad determinística de pos procesamiento está configurada para reducir el sesgo del número generado en la unidad determinística de muestreo pos procesándolo para generar un dato de salida. Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto de muestrear una fuente de entropía por medio de una segunda fuente de entropía para controlar qué datos deben ser muestreados del flujo de bits de la primera fuente de entropía y, de esta manera, obtener un número aleatorio. Sumado a lo anterior, la materia reivindicada, es susceptible de aplicación industrial.

En consecuencia, las reivindicaciones 1 a 14 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y este Despacho encuentra procedente conceder para las mismas la patente solicitada.

SÉPTIMO: Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2017/0008879 el 12 de mayo de 2020 y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: “DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA”.

Con fundamento en las anteriores consideraciones, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO PRIMERO: Otorgar patente de invención para la creación titulada:

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

Clasificación IPC: *G06F 7/58.*

Reivindicación(es): *1 a 14 incluidas en el radicado bajo el No NC2017/0008879 el 12 de mayo de 2020, de acuerdo con el anexo 1.*

Titular(es): *UNIVERSIDAD INDUSTRIAL DE SANTANDER.*

Domicilio(s): *CARRERA 27 CALLE 9 CIUDAD UNIVERSITARIA, BUCARAMANGA SANTANDER, COLOMBIA.*

Inventor(es): *Élkim Felipe ROA FUENTES, Héctor GÓMEZ.*

Resolución N° **3548**

Ref. Expediente N° NC2017/0008879

Vigente desde: *30 de agosto de 2017* ***Hasta:*** *30 de agosto de 2037.*

ARTÍCULO SEGUNDO: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO TERCERO: Notificar el contenido de la presente resolución a UNIVERSIDAD INDUSTRIAL DE SANTANDER, advirtiendo que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 3 de febrero de 2021

ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente por: ANDRES BERNARDO BARRETO GONZALEZ
Fecha: 2021.02.04 09:07:54 COT
Razón: Validez juridica.
Ubicación: Bogotá, Colombia.

Resolución N° **3548**

Ref. Expediente N° NC2017/0008879

ANEXO 1

REIVINDICACIONES CONCEDIDAS

1. Un generador de números aleatorios que comprende:
   - una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y 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;
   - 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 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);
   - 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 dato de salida.

2. El generador de números aleatorios de la Reivindicación 1, donde la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende:
   - un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b);
   - la salida del segundo multiplexor (11b) está conectada a la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas están conectadas a la entrada de un primer multiplexor (11a);
   - la salida del primer multiplexor (11a) está conectada con la entrada del primer conjunto de compuertas NAND;

   donde el primer conjunto de compuertas NAND(14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas| NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).

3. El generador de números aleatorios de la Reivindicación 1, donde la fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) conectada a un flip-flop (8), una segunda fuente de entropía interna (18b) conectada a un primer PRBS (7a) que se conecta al flip-flop (8).

4. El generador de números aleatorios de la Reivindicación 1, donde la fuente de entropía (1a) o una segunda fuente de entropía (2a) comprende: una primera fuente de

entropía interna (18a) conectada a la entrada de un primer contador (9a), una segunda fuente de entropía interna (18b) conectada a un segundo contador (9b); la salida del primer contador (9a) conectada a una de las dos entradas de un comparador digital (10) y a una entrada de un primer multiplexor (11a), la salida del segundo contador (9b) conectada a una de las entradas de un comparador digital (10) y a una entrada del primer multiplexor (11a); la salida del comparador digital (10) conectada al primer multiplexor (11a) cuya salida a su vez está conectada a un medidor de cambio de frecuencia (12a) y a un flip-flop (13).

5. El generador de números aleatorios de la Reivindicación 1, donde la fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) cuya salida está conectada a un primer medidor de cambio de frecuencia (12a) y a una de las entradas de un primer contador (9a); el primer medidor de cambio de frecuencia (12a) se conecta a su vez a una segunda fuente de entropía interna (18b) y su salida está conectada a una segunda entrada del primer contador (9a) y a un segundo medidor de cambio de frecuencia (12b) que se conecta al CLK de un flip-flop (13), y la salida del primer contador (9a) está conectada a un flip-flop (13).

6. El generador de números aleatorios de la Reivindicación 1, donde la primera fuente de entropía (1a) y la segunda fuente de entropía (2a) son intercambiables.

7. El generador de números aleatorios de la Reivindicación 1, donde la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) son arreglos de fuente de entropía y comprende: un primer conjunto de fuentes de entropía conectado a la entrada de un primer multiplexor (11a); el primer multiplexor (11a) está conectado a una unidad determinística de muestreo y posprocesamiento (15); un segundo conjunto de fuentes de entropía conectado a un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada con la unidad determinística de muestreo y posprocesamiento (15); donde el primer conjunto de fuentes de entropía va desde una primera fuente (19a) a un número (o) de fuentes de entropía (19a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un primer multiplexor (11a) y el segundo conjunto de fuentes de entropía va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b).

8. El generador de números aleatorios de la Reivindicación 1 donde la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) son arreglos de fuente de entropía y comprende: un primer conjunto de fuentes de entropía conectado a la entrada de un primer multiplexor (11a), una tercera fuente de entropía (3a) conectada a un primer PRBS (7a) y cuya salida está conectada al primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada a una de las entradas de la unidad determinística de muestreo y posprocesamiento (15); un segundo conjunto de fuentes de entropía conectado a la entrada de un segundo multiplexor (11b), una cuarta fuente de entropía (3b) conectada a un segundo PRBS (7b) y cuya salida conecta a la unidad determinística de muestreo y posprocesamiento (15), la salida del segundo multiplexor

(11b) conectada a una de las entradas de la unidad determinística de muestreo y posprocesamiento (15); donde el primer conjunto de fuentes de entropía va desde una primera fuente (19a) a un número (o) de fuentes de entropía (19a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un primer multiplexor (11a) y el segundo conjunto de fuentes de entropía va desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b).

9. El generador de números aleatorios de la Reivindicación 1 donde la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) son arreglos de fuente de entropía y comprende: un primer conjunto de fuentes de entropía se forma desde una primera fuente de entropía (19a) a un número (o) de fuentes de entropía (1a), siendo (o) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta a un primer multiplexor (11a), la salida de cada fuente de entropía (19a) conectada a cada una de las entradas del primer multiplexor (11a), una tercera fuente de entropía (3a) conectada a un primer PRBS (7a) y cuya salida está conectada al primer multiplexor (11a), la salida del primer multiplexor (11a) está conectada a un flip-flop (16); un segundo conjunto de fuentes de entropía (19b) se forma desde una segunda fuente de entropía (19b) a un número (p) de fuentes de entropía (19b), siendo (p) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b), la salida de cada fuente de entropía (19b) está conectada a cada una de las entradas del segundo multiplexor (11b), una cuarta fuente de entropía (3b) está conectada a un segundo PRBS (7b) y cuya salida está conectada al segundo multiplexor (11b), la salida del segundo multiplexor (11b) está conectada a un tercer PRBS (7c) y su salida conectada a un flip-flop (16).

10. El generador de números aleatorios de la Reivindicación 1 donde la primera fuente de entropía (1a) o la segunda fuente de entropía (2a) comprende: una primera fuente de entropía interna (18a) que conecta a un primer PRBS (7a) que conecta a un limitador (17) que a su vez está conectado a un flip-flop (16), una segunda fuente de entropía interna (18b) está conectada a un segundo PRBS (7b) cuya señal de salida está conectada a un flip-flop (16).

11. El generador de números aleatorios de acuerdo con cualquiera de las Reivindicaciones 4, 6 o 10, donde la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) se seleccionan del grupo de fuentes de entropía conformado por osciladores de anillo, *latches* metaestables, ruido térmico amplificado de una resistencia y circuitos de tiempo de captura y ruptura del óxido de un transistor bajo una tensión de estrés.

12. El generador de números aleatorios de la Reivindicación 4, donde la primera fuente de entropía interna (18a) o la segunda fuente de entropía interna (18b) comprende: un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada a la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas están

conectadas a la entrada de un primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada con la entrada del primer conjunto de compuertas NAND; donde el primer conjunto de compuertas NAND(14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).

13. El generador de números aleatorios de la Reivindicación 5, donde la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) comprende cada una: un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada a la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas están conectadas a la entrada de un primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada con la entrada del primer conjunto de compuertas NAND; donde el primer conjunto de compuertas NAND(14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).

14. El generador de números aleatorios de la Reivindicación 10, donde la primera fuente de entropía interna (18a) y la segunda fuente de entropía interna (18b) comprende cada una: un primer conjunto de compuertas NAND (14a) conectado a la entrada de un segundo multiplexor (11b); la salida del segundo multiplexor (11b) está conectada a la entrada de un segundo conjunto de compuertas NAND (14b) cuyas salidas están conectadas a la entrada de un primer multiplexor (11a); la salida del primer multiplexor (11a) está conectada con la entrada del primer conjunto de compuertas NAND; donde el primer conjunto de compuertas NAND(14a) se forman desde una compuerta NAND (14a) hasta un número (n) de compuertas NAND (14a), siendo (n) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta un segundo multiplexor (11b) y el segundo conjunto de compuertas NAND (14b) se forman desde una compuerta NAND (14b) hasta un número (m) de compuertas NAND (14b), siendo (m) un número natural mayor que cero y definido por la cantidad de entradas con las que cuenta el primer multiplexor (11a).