Señores
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
DIRECCIÓN DE NUEVAS CREACIONES
E. S. D.

Re.: Expediente No. NC2017/0008879
Solicitud de Patente de Invención titulada: "DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA"
Solicitante: UNIVERSIDAD INDUSTRIAL DE SANTANDER
Nuestra Ref.: P2017/000213

RESPUESTA AL OFICIO No. 12218,
NOTIFICADO EL 29 DE SEPTIEMBRE DE 2020
(SEGUNDO EXAMEN DE FONDO)

CARLOS R. OLARTE, mayor de edad y vecino de Bogotá, identificado tal como aparece al pie de mi firma, en mi carácter de apoderado de la sociedad solicitante, me permito manifestar lo siguiente ante el auto emanado por ese Despacho, dentro del plazo legal, previsto en el artículo 45 de la Decisión 486, en los siguientes términos:

1. a- El Despacho considera que los documentos US 2017/090872 (D2) y el documento US 2008/022039 (D3) afectan el nivel inventivo de la Reivindicaciones 1 y 6.

i) En relación con la Reivindicación 1, el Despacho considera que D2 es el estado de la técnica más cercano porque divulga un generador de números aleatorios. El Despacho considera D2 se diferencia de la presente invención en que D2 no divulga una unidad determinística de muestreo configurada para generar un número a partir de una semilla. En ese sentido, el Despacho indica que el efecto técnico de esta diferencia es generar un número aleatorio que luego es posprocesado por la unidad determinística de posprocesamiento para generar el dato de salida.

El Despacho argumenta que el problema técnico objetivo que resuelve el método reclamado es: *¿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?* Así las cosas, el Despacho argumenta que D3 divulga un generador de números aleatorios que incluye una unidad determinística de muestreo 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.

En consecuencia, el Despacho considera que una 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 de D3 en el dispositivo de D2, por lo cual la materia reclamada en la Reivindicación 1 carecería de nivel inventivo.

ii) Asimismo, el Despacho considera que la materia reclamada en la Reivindicación 6 se encuentra afectada por el nivel inventivo, al citar el párrafo 093 de D3, por lo que el Despacho considera que no tiene nivel inventivo.

b- En cuanto a mis argumentos presentados en respuesta al primer examen de fondo, el Despacho argumenta lo siguiente:

i) en cuanto a mi argumento de que D1 no divulga dos fuentes de entropía, el Despacho argumenta que D2 lo divulga en el párrafo 82, en el que se indica que RNG combina una entropía de una o más fuentes de entropía independientes para generar un número aleatorio. En otra realización, puede utilizar uno o más recursos de entropía auto calibrados para generar números aleatorios. En otra realización, RNG puede incluir circuitos extractores para generar un flujo de bits de salida a partir de sus fuentes de entropía. Así mismo, D3 en el párrafo 91 divulga que las mediciones de tiempo de acceso al disco pueden mezclarse con las mediciones derivadas de la otra fuente de entropía, y que es conocida. La fuente, según D3, es una fuente de números variables que pueden ser bits individuales, derivados de la medición de un fenómeno físico que tiene grado de aleatoriedad;

ii) en cuanto a mi argumento de que D1 no divulga una primera fuente de entropía conectada a la primera entrada de una unidad determinística de muestreo, el Despacho argumenta que tanto D2 como D3 mencionan diferentes fuentes de entropía, y por lo tanto, 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.

c- En cuanto a la objeción de nivel inventivo elevada por el Despacho, si bien es cierto que el arte previo citado divulga características similares con la presente invención, el Despacho pasa por alto características importantes de la presente invención a la luz del arte previo citado.

i) En primer lugar, la presente invención corresponde a 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 con distribución estadística cercana a la uniforme. Además, el generador de números aleatorios tiene una primera fuente de entropía (1a) conectada a la primera entrada de la 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 determinística de muestreo (3).

Adicionalmente, la invención de la Reivindicación 1 tiene 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) posprocesándo dicho número para generar un dato de salida.

ii) En cuanto al arte previo, respetuosamente me permito señalar que D2 corresponde a un método y a un sistema de generación de números aleatorios que comprende un procesador con una unidad de ejecución que genera números aleatorios.

D2 divulga un sistema 1800 para la generación de números aleatorios. El sistema 1800 puede incluir un procesador 1806 y un generador de números aleatorios (RNG) 1828. El RNG 1828 puede implementarse, por ejemplo, mediante circuitos o una combinación de circuitos y bloques lógicos. Además, el RNG 1828 puede seleccionarse del grupo de generadores de números aleatorios que comprende: generadores de números aleatorios de entropía completa, generadores verdaderos de números aleatorios y generadores ligeros de números aleatorios. Similarmente, el RNG 1828 puede incluir y combinar una o más fuentes de entropía seleccionadas del grupo de fuentes de entropía: fuentes de entropía totalmente digitales, fuentes de entropía independientes, y fuentes de entropía autocalibradas.

En una modalidad de D2, el RNG 1828 puede incluirse en el procesador 1806, por ejemplo, en una unidad de ejecución 1822, dentro de un conducto de ejecución en orden o fuera de orden 1816. En otra modalidad de D2, el RNG 1828 puede ser colocado junto con un procesador en un chip, pero puede ser una entidad autónoma. A continuación, se ilustra en la FIG. A (graficada a partir de la FIG. 9 de D2) el procesador 1806 en color amarillo, el generador de números aleatorios RNG 1828 en color verde y la unidad de ejecución 1822 en color azul.

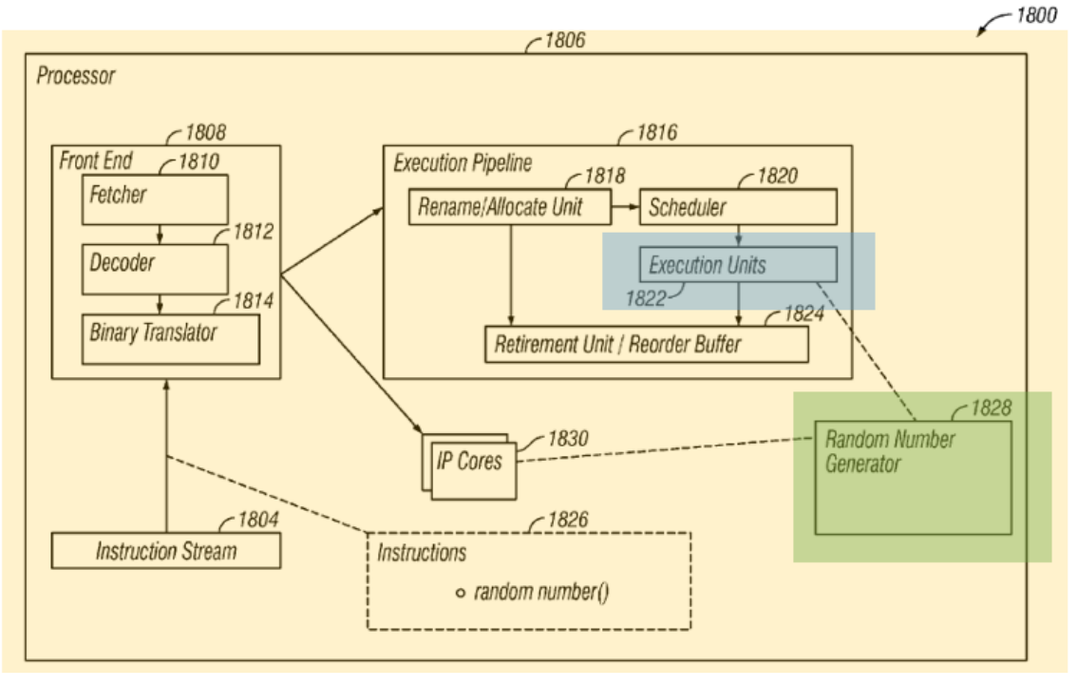


FIG. A

De la misma manera, D2 divulga un generador de números aleatorios RNG 1900 que puede implementar, total o parcialmente, el RNG 1828. Además, el RNG 1900 puede incluir una o varias fuentes de entropía totalmente digitales 1904, 1906, 1908, supresores de correlación para cada fuente de entropía 1910, 1912, 1914, y un extractor 1920 conectado a los supresores de correlación. Las fuentes de entropía de 1904, 1906, 1908 pueden compartir un suministro de voltaje y un reloj comunes, y producir cada una un bit por ciclo de reloj. El resultado puede ser tres flujos de bits brutos independientes. Los supresores de correlación 1910, 1912, 1914 pueden ejecutar una transformación que reduzca una posible dependencia estadística de las fuentes y generar cada una de ellas una cadena de 8 bits sin correlación cada 64 ciclos de reloj. El extractor 1820 puede realizar cualquier cálculo adecuado para extraer un conjunto aleatorio de valores de las cadenas no correlacionadas de 8 bits cada 64 ciclos.

A continuación, se ilustra en la FIG. B (graficada a partir de la FIG. 10 de D2) las fuentes de entropía en color azul, los supresores de correlación en color verde y el extractor en color anaranjado.

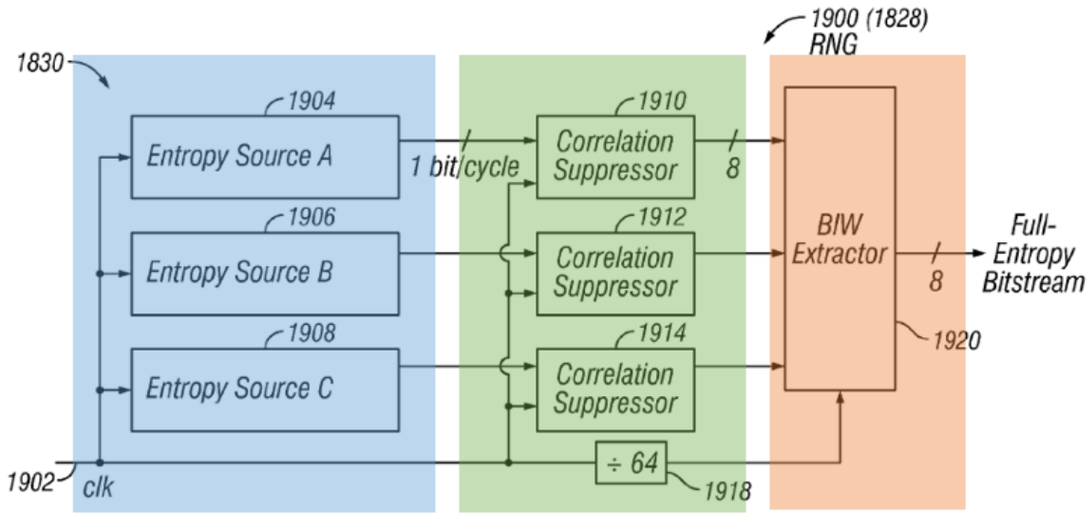


FIG. B

Por otro lado, D3 divulga un método y un controlador para generar números aleatorios mediante la alineación de un conjunto de mediciones de tiempos de acceso a direcciones aleatorias de una unidad de disco duro.

El método gestiona la generación de una dirección aleatoria en la unidad de disco duro, el acceso a la dirección aleatoria generada, la medición del tiempo de acceso y la realización de un proceso de alineación del conjunto de mediciones de tiempo de acceso para obtener un número aleatorio.

De la misma forma, el controlador incluye: un generador de números pseudo-aleatorio 16, un generador de direcciones aleatorias de la unidad de disco a partir del generador de números pseudo-aleatorios 16, una unidad de control 10 para acceder a la unidad de disco a una dirección generada por el generador de direcciones, un temporizador 15 para medir el tiempo que tarda acceder al disco, un alineador para corregir las mediciones de tiempo de acceso al disco y así obtener un número aleatorio. A continuación, se ilustra en la FIG. C (graficada a partir de la FIG. 2 de D2) el aparato de cómputo 20 en color gris, el generador de números pseudo-aleatorios 16 en color amarillo, el temporizador 15 en color verde, la unidad de control 14 en color azul y la unidad de disco duro 1 en color rojo.

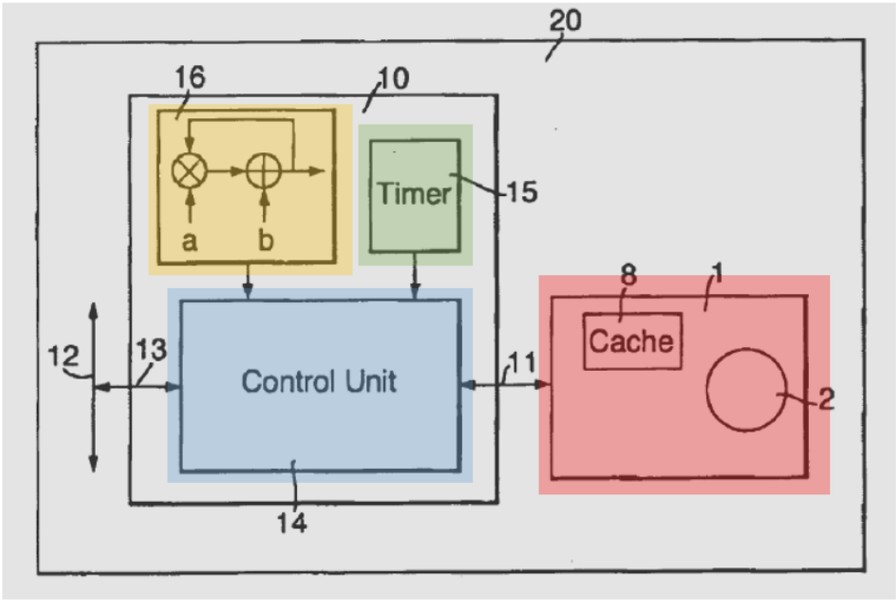


FIG. C

Así mismo, D3 enseña que el proceso de alineación reduce el sesgo y la correlación en la salida de la fuente de entropía. En una modalidad de la invención, el proceso de alineación puede realizarse mediante una operación de OR exclusivo sobre el conjunto de mediciones del tiempo de acceso al disco.

Similarmente, D3 divulga una fuente de entropía que puede utilizar las mediciones del tiempo de acceso a las direcciones aleatorias en el disco duro para generar números aleatorios. En una modalidad de la invención, la fuente de entropía puede combinarse con otras fuentes de entropía disponibles en el aparato informático 20.

Por último, D3 divulga que los números aleatorios generados por el controlador 10 pueden usarse como semilla de un generador de números pseudoaleatorios para generar una secuencia más larga de números aleatorios. Además, el generador de números pseudoaleatorios puede incorporarse en el controlador 10 u otro componente del aparato informático 20.

Ahora bien, después de haber definido el alcance de la presente invención y haber descrito el arte previo citado, me permito realizar el análisis de nivel inventivo de acuerdo con la Guía para Examen de Solicitudes de Patente y Modelos de Utilidad de la SIC (en adelante, Guía de la SIC)[1]. La Guía de la SIC señala que "*Durante el examen de nivel inventivo debe hacerse un juicio de valor y un análisis objetivo de las divulgaciones previas del estado de*

[1] Superintendencia de Industria y Comercio, *op. cit.*, sección 2.13.5, páginas 131-134

la técnica, no influenciados por el conocimiento que ya se tiene de la Invención que se está evaluando. Por tanto, con el fin de minimizar la subjetividad y evitar que se realice un análisis en retrospectiva ("hindsight" ó "a posteriori"), el examen debe relacionar la invención con la solución de un problema técnico, mediante el Método "problema-solución" (énfasis fuera de texto).

iii) **Análisis de nivel inventivo de la Reivindicación 1:**

A. Identificar el estado de la técnica más cercano a la invención reivindicada

El estado de la técnica más cercano a la invención de la Reivindicación 1 es D2, en cuanto a que divulga características similares a las reclamadas en la Reivindicación 1, y pertenece al mismo campo técnico. Particularmente, D1 divulga un procesador con una unidad de ejecución para generar un número aleatorio.

B. Determinar la diferencia entre la invención y el estado de la técnica más cercano

La Reivindicación 1 se diferencia de D2, en cuanto a que éste documento citado por el Despacho no divulga las siguientes características de la invención:

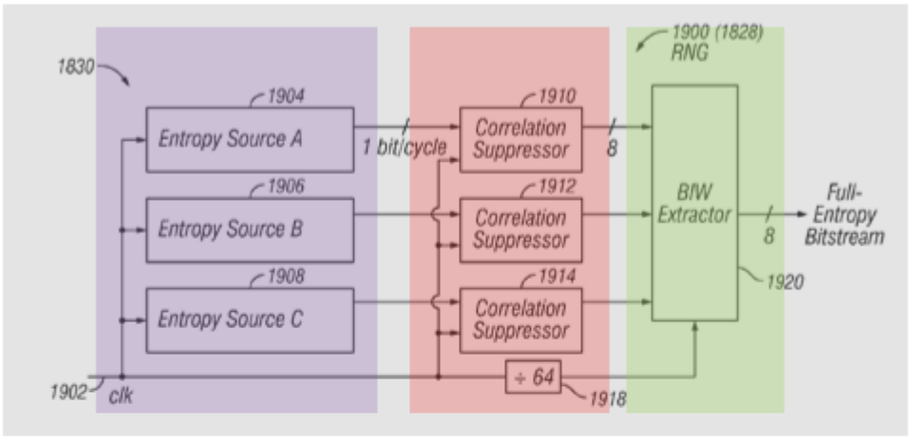
- D2 no divulga una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y una salida, donde **la unidad determinística de muestreo (3) está configurada para generar a partir de una semilla un número compuesto de números con distribución estadística cercana a la uniforme;**

El Despacho se equivoca al argumentar que D2 divulga una unidad determinística de muestreo (3) con una primera entrada, una segunda entrada y una salida. Por el contrario, D2 enseña un extractor 1920 que toma los datos de los supresores de correlación 1910, 1912, 1914 y mediante cualquier cálculo adecuado puede extraer un conjunto aleatorio de valores a partir de las cadenas no correlacionadas resultantes de los supresores de correlación 1910, 1912, 1914. Sin embargo, la unidad determinística de muestreo de la presente invención toma los datos directamente de las fuentes de entropía y muestrea los datos del flujo de bits de la primera fuente de entropía según las indicaciones de la semilla proporcionada por la segunda fuente de entropía. Por lo tanto, la unidad determinística de la

presente invención no extrae un conjunto de datos a partir de varios flujos de bits aleatorios resultantes de los supresores de correlación según diferentes cálculos.

Similarmente, el Despacho se equivoca en su argumentación porque, contrario a la presente invención, D2 divulga que varias fuentes de entropía 1904, 1906, 1908 pueden combinarse para generar un solo flujo de bits. Sin embargo, los flujos de bits de las dos fuentes de entropía de la presente invención no se combinan. Por el contrario, los datos del flujo de bits que se obtiene al muestrear el flujo de bits de la primera fuente de entropía (1a) mediante la unidad determinística de muestreo (3) corresponden solo a datos generados por dicha fuente de entropía, es decir que ninguno de los datos corresponde a datos del flujo de bits de la segunda fuente de entropía (2a). Mientras que en D2, los flujos de bits generados por cada una de las fuentes de entropía son combinados por un extractor para obtener un solo flujo de bits a la salida. Adicionalmente, el Despacho se equivoca al argumentar que D2 divulga que la segunda fuente de entropía (2a) está configurada para proporcionar la semilla a la unidad determinística de muestreo (3). Por el contrario, los flujos de bits de cualquiera de las fuentes de entropía de D2 son usados de manera indistinta como datos de entrada al extractor. Sin embargo, la segunda fuente de entropía (2a) de la presente invención está configurada para proporcionar la semilla a unidad determinística de muestreo (3), donde la semilla corresponde a un parámetro de control. Es decir, que la unidad determinística de muestreo no retorna ninguno de los datos de semilla proporcionados por la segunda fuente de entropía (2a) y dichos datos de semilla tampoco son combinados con los datos de la primera fuente de entropía (1a).

Además, el Despacho se equivoca al argumentar que D2 divulga dos fuentes de entropía conectadas a una unidad determinística de muestreo. Por el contrario, D2 divulga que las fuentes de entropía 1904, 1906, 1908 alimentan directamente un supresor de correlación 1910, 1912, 1914 por cada fuente de entropía para eliminar la correlación proveniente de dichas fuentes de entropía. Sin embargo, las fuentes de entropía de la presente invención alimentan una unidad determinística de muestreo que permite muestrear la primera fuente de entropía (1a) a partir de la segunda fuente de entropía (2a). A continuación, se presentan en la FIG. C las diferencias mencionadas, así: el dispositivo de D2 en color gris oscuro con las fuentes de entropía en color morado, los supresores de correlación en color rojo y el extractor en color verde; de la misma manera, el dispositivo de la presente invención en gris claro con la primera fuente de entropía (1a) en color morado, la segunda fuente de entropía (2a) en color amarillo, la unidad determinística de muestreo en color verde y la unidad de posprocesamiento en color rojo.



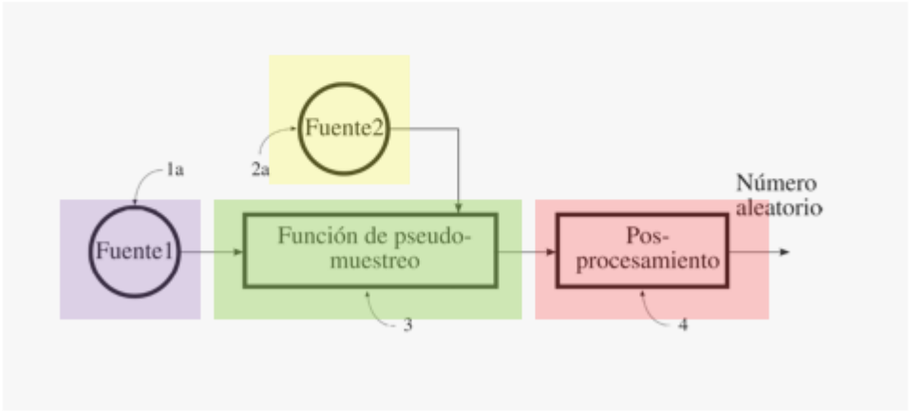


FIG. C

- **<u>D2 no divulga una primera fuente de entropía (1a) conectada a la primera entrada de la unidad determinística de muestreo (3);</u>**

El Despacho se equivoca al argumentar que D2 divulga una primera fuente de entropía conectada a una unidad determinística de muestreo. Por el contrario, D2 divulga que, antes de conectar las fuentes de entropía 1904, 1906, 1908 al extractor 1920, cada una de las fuentes de entropía se conecta a su respectivo supresor de correlación 1910, 1912, 1914. Sin embargo, tanto la primera como la segunda fuente de entropía de la presente invención se conectan directamente a la unidad determinística de muestreo (3) sin que el flujo de bits que ellas generan pase por supresores de correlación.

- D2 no divulga 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), **<u>donde la segunda fuente de entropía (2a) está configurada para proporcionar la semilla a la unidad determinística de muestreo (3);</u>**

El Despacho se equivoca al argumentar que D2 divulga 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). Por el contrario, D2 divulga que cada una de las fuentes de entropía se conecta a un supresor de correlación antes de conectarla al extractor. Sin embargo, la segunda fuente de entropía (2a) de la presente invención se conecta a la unidad determinística de muestreo (3). Más aún, el Despacho se equivoca al argumentar que D2 divulga que la segunda fuente de entropía (2a) está configurada para proporcionar la semilla a la unidad determinística de muestreo (3). Por el contrario, las fuentes de entropía D2 son empleadas para combinar sus respectivos flujos de bits en el extractor 1920, sin que alguna de ellas esté configurada para proporcionar una semilla al extractor 1920 o a una unidad determinística de muestreo (3). Sin embargo, la segunda fuente de entropía (2a) de la presente invención proporciona el flujo de bits de semilla que requiere la unidad determinística de muestreo (3) para determinar qué datos del flujo de bits de la primera fuente de entropía debe muestrear.

- D2 no divulga 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.

El Despacho se equivoca al argumentar que D2 divulga una unidad determinística de posprocesamiento (4) conectada a la salida de la unidad determinística de muestreo (3). Por el contrario, D2 divulga que los flujos de bits generados por las fuentes de entropía primero ingresan a los supresores de correlación correspondientes. De manera posterior, los supresores de correlación generan un flujo de bits intermedio que ingresa al extractor 1920. Sin embargo, la unidad de posprocesamiento de la presente invención no está conectada directamente a las fuentes de entropía sino que está conectada a la unidad determinística de muestreo. Por lo tanto, los datos que ingresan a la unidad de posprocesamiento han sido procesados por la unidad determinística de muestreo y no corresponden de forma exacta a los datos generados por alguna de las fuentes de entropía, sino que corresponden a los datos muestreados de la primera fuente de entropía según los datos de semilla proporcionados por la segunda fuente de entropía mediante la unidad determinística de muestreo.

Además, el Despacho se equivoca al argumentar que D2 divulga que 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. Por el contrario, D2 divulga un supresor de correlación 1910, 1912, 1914 conectado que recibe los datos de las fuentes de entropía y genera un bit sin correlación por cada 8 bits que recibe de la fuente de entropía. Sin embargo, la unidad determinística de posprocesamiento del presente invento está conectada a la salida de la unidad determinística de muestreo y recibe el flujo de bits aleatorios generados por unidad determinística de muestreo más no recibe de forma directa los bits que generan las fuentes de entropía. Es decir, que la presente invención elimina el sesgo luego de generado el número aleatorio, en comparación con D2 que elimina el sesgo directamente de las fuentes de entropía.

C. Definir el efecto técnico causado y atribuible al elemento diferencial

De acuerdo con lo anterior, uno de los efectos técnicos asociados a las diferencias entre el arte previo citado por el Despacho y la invención de la Reivindicación 1 está dado por la unidad determinística de muestreo que incluye el generador de números aleatorios de la presente invención. La unidad determinística de muestreo permite muestrear una fuente de entropía por medio de una segunda fuente de entropía. Para lo anterior, la unidad determinística de muestreo emplea una semilla, dada por el flujo de bits de la 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.

Adicionalmente, otro de los efectos técnicos asociados a las diferencias entre el arte previo citado por el Despacho y la invención de la Reivindicación 1 es que la unidad determinística de posprocesamiento recibe los números aleatorios de la unidad determinística de muestreo y reduce el sesgo de la cadena de números aleatorios.

D. Deducir el problema técnico a solucionar

En cuanto a esta etapa del método problema-solución, el Despacho se equivoca al afirmar que el problema que resuelve la invención es *¿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?*, pues como se dijo anteriormente hay más diferencias entre la invención aquí reclamada y D2, a la generación de un número aleatorio que luego es posprocesado por la unidad determinística de posprocesamiento para generar el dato de salida.

Por otra parte, me permito señalar que la Guía de la SIC establece que el problema técnico debe ser formulado de la siguiente manera: *"¿cómo modificar o adaptar el estado de la técnica cercano para obtener el efecto técnico que la invención proporciona?"*. Adicionalmente, me permito aclarar que de acuerdo con el Manual Andino de Patentes (MAP) *"se debe definir el problema* ***sin incluir elementos de la solución****, porque entonces la solución sería evidente"* (énfasis fuera del texto).

Con base en lo anterior, uno de los problemas técnicos asociados a los efectos técnicos de las diferencias, se podría formular de la siguiente manera ¿cómo modificar a D2 para que alguna de las fuentes de entropía sea la semilla de la unidad determinística de muestreo que seleccione los datos, de la primera fuente de entropía, a procesar por la unidad determinística de posprocesamiento?

E. Evaluar si la invención reivindicada, partiendo del estado de la técnica cercano y del problema técnico objetivo, habría sido obvia para la persona medianamente versada en la materia

i) En este punto me permito nuevamente resaltar la Guía de la SIC que establece: *"esta etapa consiste en responder a la pregunta de si en el estado de la técnica en su conjunto hay un segundo documento que contiene una enseñanza que indicaría* ***(no sólo que podría indicar, sino que indicaría)*** *a la persona medianamente versada en la materia, enfrentada al problema técnico, cómo modificar o adaptar el estado de la técnica más cercano para resolver el problema, de la forma reivindicada"* (énfasis fuera del texto).

Así, el análisis de nivel inventivo de solicitudes de patente, no se trata de encontrar en el arte previo una mera invitación a experimentar con uno o más cambios aleatorios, sino de identificar en los documentos citados una enseñanza y guía específica para hacer las modificaciones necesarias y no otras que lo lleven con certeza a la materia reclamada.

Evidentemente, el arte previo citado por el Despacho no brinda las enseñanzas suficientes para que la persona medianamente versada en la materia desarrolle inequívocamente la presente invención y mucho menos espere la obtención de los resultados señalados. Particularmente, el Despacho argumenta que D2 divulga todas las características esenciales de la presente invención excepto que la generación de números aleatorios se realice a partir de una semilla. Por otro lado, el Despacho argumenta que D3 divulga que el número aleatorio generado por el controlador puede usarse como semilla de un generador de números pseudoaleatorios para generar una secuencia más larga de números aleatorios, razón por la que el Despacho argumenta que esta característica de D3 es la característica

faltante en D2 y que al combinarse con las enseñanzas de D2 se puede obtener la presente invención. Sin embargo, las características esenciales de la presente invención no se encuentran divulgadas en D2.

Similarmente, el Despacho se equivoca al argumentar que la característica faltante en D2 se divulga en D3, puesto que en realidad D3 divulga que en una modalidad de la invención un número aleatorio generado por una fuente de entropía puede ser usado como semilla de un generador pseudoaleatorio para generar una secuencia más larga de números aleatorios. Es decir que, el número aleatorio de la semilla divulgada en D3 corresponde a un número inicial a partir del cual se construye una secuencia más larga de números aleatorios.

Por el contrario, en el presente invento, la unidad determinística tiene dos fuentes de entropía donde la segunda fuente de entropía muestrea la primera fuente. La segunda fuente de entropía genera un flujo de bits aleatorio e independiente del flujo de bits de la primera fuente de entropía, el cual es la semilla que recibe la unidad determinística de muestreo. El flujo de bits de la semilla le indica a la unidad determinística de muestreo cuales son los datos que debe muestrear del flujo de bits de la primera fuente de entropía. De esta forma, la semilla es un indicador para la unidad determinística de muestreo, pero el flujo de bits resultante de esta unidad corresponde al flujo de bits muestreado de la primera fuente de entropía. Es decir, que no se está generando un número aleatorio a partir de una semilla como en el caso de D3, sino que por el contrario la semilla determina que datos muestrear del flujo de bits de la primera fuente de entropía. Por lo tanto, el concepto de semilla es diferente que el citado por el Despacho.

Adicionalmente, el arte previo citado no divulga ninguna enseñanza, motivación o sugerencia que le indique a una persona medianamente versada en la materia que para obtener un número aleatorio debe muestrear el flujo de bits de una primera fuente de entropía mediante una unidad determinística de muestreo controlada por una semilla suministrada por el flujo de bits de una segunda fuente de entropía, y mucho menos se encuentra un indicio que le indique a la persona medianamente versada en la materia que después de hacer esto, debe reducir el sesgo de la cadena aleatoria proveniente de la unidad determinística de muestreo mediante una unidad de posprocesamiento.

Por el contrario, a partir del arte previo citado por el Despecho una persona medianamente versada en la materia estaría motivada a combinar varias fuentes de entropía que generen un número aleatorio mediante el procesamiento de un conjunto de mediciones de tiempo de acceso a un disco duro. Así mismo, la persona medianamente versada en la materia estaría motivada a emplear el número aleatorio, generado por la combinación de las fuentes de

entropía, como número inicial (semilla) de un generador de números pseudo-aleatorios para generar una cadena más larga de números aleatorios.

Así las cosas, me permito señalar que se debe reconocer que las diferencias en las dimensiones del método del presente invento muestran un efecto técnico inesperado y ventajoso a la luz de la técnica anterior, como se indicó anteriormente y como lo requiere la Guía de Examen de solicitudes de patentes y modelos de utilidad de la SIC.[2]

ii) En consecuencia, y a la luz de las evidentes diferencias encontradas entre la materia reclamada en la solicitud frente al arte previo, vale la pena señalar que de acuerdo con el MAP, para que pueda negarse la existencia de nivel inventivo, es necesario, no solamente que la combinación de las enseñanzas pueda hacerse, sino también que exista una sugerencia o razón tal, que lleve a la persona medianamente versada en la materia a combinar las enseñanzas de los documentos[3]. De manera similar, la Guía de la SIC establece que, para que una invención no resulte inventiva "*el conjunto de enseñanzas del estado de la técnica lo llevarían* (a la persona medianamente versada en la materia) *de forma inmediata a la solución propuesta por la solicitud.* ***Si se requiere de pasos adicionales o de corroboración o de superar obstáculos revelados por las propias enseñanzas entonces el estado de la técnica no revela la solución al problema***"[4] (énfasis fuera del texto). En el presente caso, las características y disposición de la presente invención no pueden predecirse a partir del arte previo que menciona el Despacho.

iii) Ahora bien, si bien el Despecho objeta el nivel inventivo de la Reivindicación dependiente 6, me permito señalar que ésta es dependiente de la Reivindicación 1 por lo tanto hereda todas sus características novedosas e inventivas. Específicamente, la Guía de la SIC establece que "*una reivindicación dependiente es la que contiene todas las características de la reivindicación de la cual depende y además: i) hace referencia a ésta; y ii) adiciona una o más características que limitan el objeto a proteger*"[5] (énfasis fuera del texto). De acuerdo con lo anterior, la Reivindicación 6, así como todas las reivindicaciones que dependen de la Reivindicación 1, al incluir las características no obvias de la Reivindicación independiente 1, son inventivas a la luz del arte previo citado.

---

[2] Superintendencia de industria y comercio de Colombia, Guía para Examen de solicitudes de Patente de Invención y Modelo de Utilidad, 2014, sección 3.5.5
[3] Comunidad Andina de Naciones, *op. cit.*, Sección 10.2.1 - Ejemplo 1
[4] Superintendencia de industria y comercio de Colombia, Guía para Examen de solicitudes de Patente de Invención y Modelo de Utilidad, 2014, sección 2.13.2
[5] Ibídem, Sección 2.6.4.2

D3 al no ser un documento que sea cercano al campo técnico del presente invento (pues no genera números aleatorios sino pseudo-aleatorios y, además, la semilla que utiliza hace referencia a un dato inicial a partir de cual se generan más números pseudo-aleatorios, más no a un dato de control que indica que datos muestrear de una primera fuente de entropía por medio de una segunda fuente), no existiría alguna o motivación en la persona medianamente versada en la materia en modificar parámetros de D3 o combinar sus enseñanzas con las de D2 se obtenga el desarrollo de la presente invención.

iv) En conclusión, la presente invención es inventiva a la luz del arte previo citado, pues siguiendo las enseñanzas de D2 y D3, la persona medianamente versada en la materia no obtendría la materia reclamada, ni podría esperar que ésta presentase las propiedades que en efecto reviste.

2. Finalmente, respetuosamente considero que la presente solicitud cumple con los requisitos de patentabilidad establecidos por la Decisión 486 y por consiguiente solicito respetuosamente que el Despacho proceda con la concesión de la patente.

Atentamente,

CARLOS R. OLARTE
C.C. No. 79.782.747 de Bogotá
T.P. 74.295