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. 2271,
NOTIFICADO EL 14 DE FEBRERO DE 2020
(PRIMER 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. En primer lugar, con el ánimo de brindar mayor claridad a la materia reivindicada, me permito presentar un **Capítulo Reivindicatorio Modificado** que reemplaza el Capítulo Reivindicatorio presentado al momento de radicar la solicitud de patente.

a) Así entonces, el Capítulo Reivindicatorio Modificado adjunto contiene los siguientes cambios:

- se modifica la Reivindicación 1 de la siguiente manera:
  - se aclara que 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, lo cual encuentra soporte en la Página 13, Párrafo 14 del Capítulo Descriptivo;
  - se especifica que la segunda fuente de entropía (2a) es independiente de la primera fuente de entropía (1a), y está configurada para proporcionar la semilla a la unidad determinística de muestreo (3), lo cual encuentra soporte en la Página 5, Párrafos 5 y 6 del Capítulo Descriptivo; y

- se aclara 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, lo cual encuentra soporte en la Página 14, Párrafo 1 y Página 6, Párrafo 2 del Capítulo Descriptivo;

- se eliminan las antiguas Reivindicaciones 5 y 7, se modifica la nueva Reivindicación 11 (antigua Reivindicación 13) de manera que ahora depende de cualquiera de las nuevas Reivindicaciones 4, 6, o 10 (antiguas Reivindicaciones 4, 6 y 12), y se reenumera el Capítulo Reivindicatorio de acuerdo con estos cambios, lo cual encuentra soporte en el Capítulo Reivindicatorio originalmente presentado.

Valga anotar que las modificaciones efectuadas en el Capítulo Reivindicatorio cumplen a cabalidad con lo estipulado en el Artículo 34 de la Decisión 486, ya que éstas de ninguna manera implican una ampliación de la protección correspondiente a la divulgación contenida en la solicitud de patente originalmente presentada. Éstas por el contrario corresponden a una limitación de la materia reclamada.

2. a- El Despacho objeta la Claridad de las Reivindicaciones de la siguiente manera:

- La Reivindicación 1 incluye la frase *"una unidad determinística de muestreo"* que sugiere un modelo matemático, lo cual no corresponde a materia patentable; y
- las Reivindicaciones 5, 7 y 13 describen los mismos elementos, por lo cual repiten la misma materia.

b- i) En cuanto a la objeción de Claridad de la Reivindicación 1, me permito respetuosamente resaltar que el término *"determinística"* no debe interpretarse de manera aislada como lo hace el Despacho, sino, que debe entenderse en el contexto del término *"unidad determinística de muestreo",* y tomando como referencia el Capítulo Descriptivo de la solicitud de patente. El término *"unidad determinística de muestreo",* corresponde a una unidad de hardware, por ejemplo, un comparador digital, donde sus salidas se conocen y son predecibles si se conocen las entradas.

De acuerdo con lo anterior, es impreciso decir que el término *"determinística",* analizado en el contexto de la expresión *"unidad* ***determinística*** *de muestreo"* sugiere un modelo matemático, pues claramente el término *"unidad"* implica que se hace referencia a un elemento de hardware, que tiene conexiones como la primera entrada, segunda entrada y

salida, las cuales se relacionan con otras características estructurales de la Reivindicación 1 en expresiones como *"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)"****, y* ***"****una unidad determinística de posprocesamiento (4)* ***conectada a la salida de la unidad determinística de muestreo (3)".***

Particularmente, me permito respetuosamente resaltar que el Capítulo Descriptivo, en la página 4 menciona que *"Para el entendimiento de la presente invención, se entenderá como* ***unidad determinística aquella función que su salida es totalmente predecible si se conocen sus entradas*** *y un ejemplo de la realización de una unidad determinística es un comparador digital".* Por lo tanto, el Capítulo Descriptivo explica de manera clara que una *"unidad determinística",* es un elemento de hardware, mas no un término alusivo a un modelo matemático.

De acuerdo con lo anterior, los términos de las Reivindicaciones deben interpretarse a la luz del Capítulo Descriptivo, y tomando en cuenta lo que entiende una persona medianamente versada en la materia por estos términos, y no deben fraccionarse para interpretar palabras de manera aislada.

En consecuencia, con base en las aclaraciones anteriores el término objetado por el Despacho es claro, por lo cual considero superada esta objeción.

ii) En relación con la objeción del Despacho respecto a las Reivindicaciones 5, 7 y 13 respecto a que estas describen los mismos elementos, me permito respetuosamente llamar la atención sobre los cambios hechos en el Capítulo Reivindicatorio Modificado adjunto, en el cual se han eliminado las antiguas Reivindicaciones 5 y 7, y se ha modificado la nueva Reivindicación 11 (antigua Reivindicación 13) de manera que ahora depende de cualquiera de las nuevas Reivindicaciones 4, 6, o 10 (antiguas Reivindicaciones 4, 6 y 12). De acuerdo con lo anterior, considero superada esta objeción.

3. a- i) El Despacho considera que el documento US 2016/0204781 (D1) afecta la novedad de las Reivindicaciones 1 a 3, 5, 7, 8 y 13.

El Despacho señala que D1 divulga sistemas y métodos para generar cadenas de bits aleatorias y, más particularmente, funciones físicamente no clonables.

El Despacho señala que D1 divulga un controlador LC LFSR (1104) que puede ser un registro de desplazamiento de retroalimentación lineal de 32 bits (LFSR) utilizado para producir unos vectores de lanzamiento aleatorio. Además, el Despacho indica que en D1 se encuentra un Controlador REBEL (1106) que puede configurar un punto de inserción (IP) en una fila REBEL asociada a la salida del bloque lógico AES.

Similarmente, en su análisis el Despacho encuentra en D1 un motor de análisis de muestras (SAE) (1108) que puede analizar 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.

Además, el Despacho señala que en D1, 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 una 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.

Asimismo, el Despacho indica que D1 divulga que las variaciones eléctricas introducidas por las variaciones del proceso definen la fuente de entropía en la que se basan las PUF. Además, el Despacho señala que en D1, 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. El 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.

En su análisis, el Despacho menciona fuentes de entropía que 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 más. Similarmente, el Despacho señala que en D1 se describe una técnica desarrollada llamada "Recuento de PN dual" (DPNC) que procesa posteriormente las PN para eliminar este sesgo. La técnica aplica una operación de módulo a los paquetes de números (PN), que "recorta" los bits de orden superior de la medición de retardo de ruta.

De acuerdo con lo anterior, el Despacho considera que la Reivindicación 1 carece de novedad a la luz de D1.

ii) En cuanto a las Reivindicaciones dependientes, el Despacho afecta su novedad citando a D1 de la siguiente manera:

- Reivindicación 2, párrafos 0150 y 0014, y Fig. 2;
- Reivindicación 3, párrafos 0048 y 0062, y Fig. 2;
- Reivindicaciones 5, 7 y 13, párrafo 0050;
- Reivindicación 8, párrafos 0122 y 0155, y Figs. 28A, 28B,

b- i) En relación con las objeciones de novedad elevadas por el Despacho, en primer lugar, llamo respetuosamente la atención del Despacho sobre las modificaciones realizadas en el Capítulo Reivindicatorio Modificado adjunto, tal como se explica en el punto 1 del presente memorial.

Ahora bien, me permito señalar que el alcance de la nueva Reivindicación 1 estaría dirigido 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 compuesto de números 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 D1 corresponde a un sistema para generar una cadena de bits para una función físicamente no clonable (PUF). D1 divulga que el HELP PUF se integra en una unidad funcional

existente, como el Estándar de cifrado avanzado (AES) (por ejemplo, una con nueve esquinas temperatura-voltaje) lo cual permite aprovechar una gran fuente de entropía mientras minimiza su huella general. Esta gran fuente de entropía permite que HELP genere cadenas de bits largas, a la vez que es conservador en los caminos seleccionados para la generación de bit. A continuación, se ilustra en la FIG. A (graficada a partir de la FIG. 1 de D1) el HELP PUF en color morado y la unidad funcional existente en color azul.

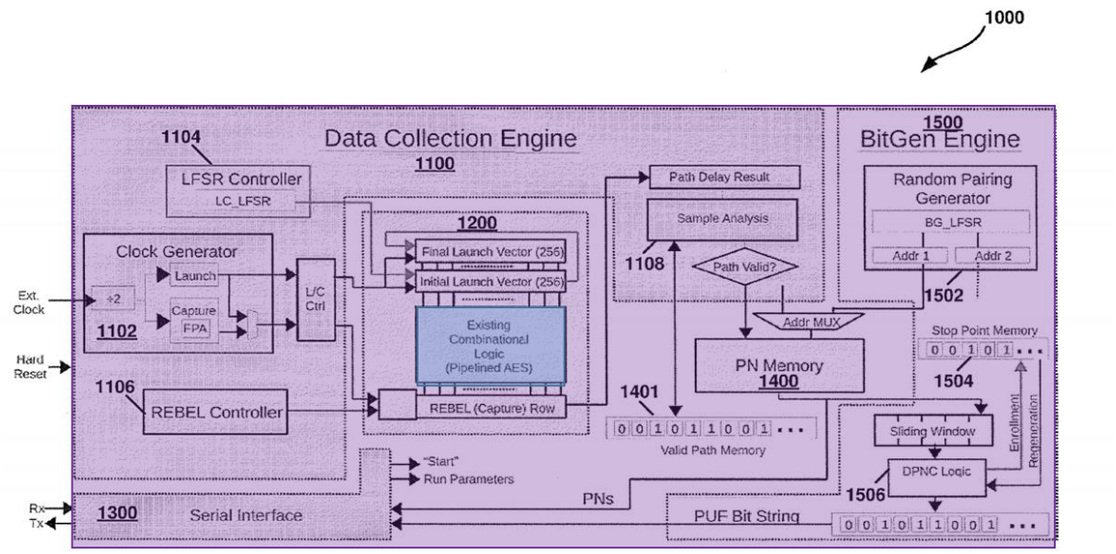

FIG. A

D1 divulga una estructura REBEL que tiene una primera cadena de escaneo de flip-flops operables acoplada a la macro bajo prueba, en la que la primera cadena de exploración está configurada para iniciar transiciones en la macro bajo prueba; y una segunda cadena de exploración de flip-flops, operable acoplada a la macro bajo prueba en donde la segunda cadena de exploración está configurada *para capturar transiciones que se propagan a través de la macro bajo prueba (MUT).* A continuación, se identifica la estructura REBEL en color verde en la FIG. B (graficada a partir de la FIG. 1 de D1):

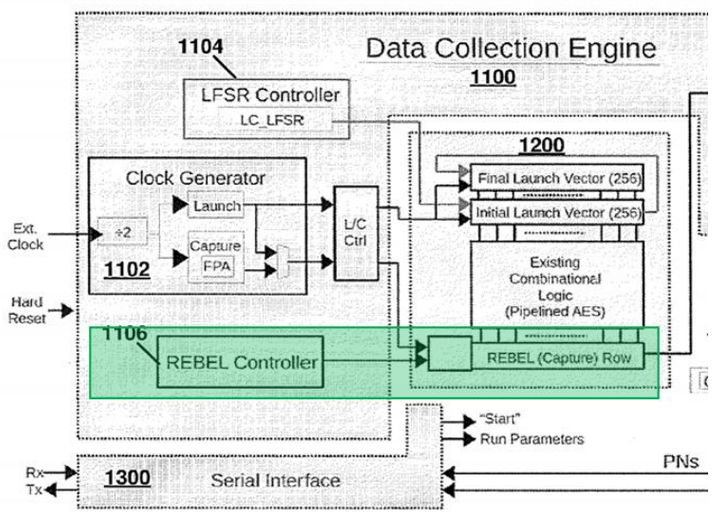

FIG. B

La estructura REBEL permite obtener representaciones digitalizadas de alta precisión de los retrasos entre los caminos lógicos. La estructura REBEL tiene una fila superior 2100, que es la fila de lanzamiento, y está configurada para funcionar en modo funcional. Además, la estructura REBEL tiene una segunda fila 2200, que es la **fila de captura**, y se configura en "modo mixto", en el que se elige un flip-flop (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" y forman una cadena de retardo combinacional, extendiendo efectivamente la ruta en el IP. A continuación, en la FIG. C (graficada a partir de la FIG. 2 de D1) se identifica la fila superior 2100 en color rosa y la segunda fila 2200 en color naranja de la estructura REBEL:

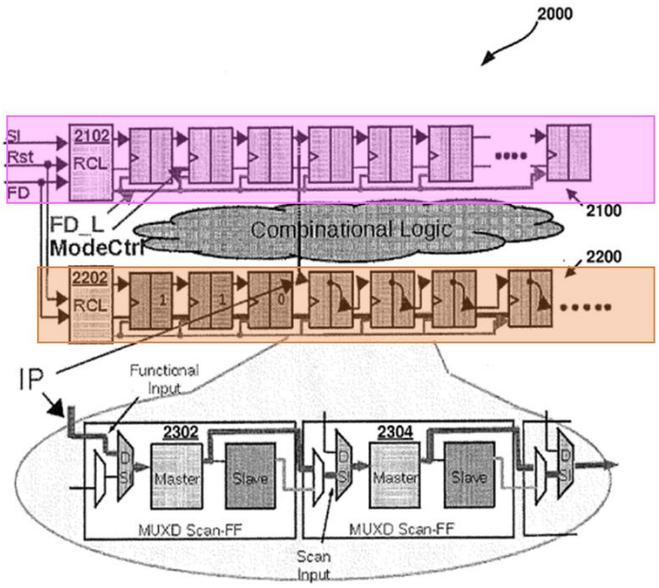

FIG. C

Además, D1 divulga que 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 pseudo aleatorio.** El proceso de D1 comienza cargando el LC LFSR con **una semilla (proporcionada por el usuario)** e instruyendo al controlador LC LFSR 1104 para cargar un par aleatorio de vectores en las filas de lanzamiento. Asimismo, D1 divulga un módulo de generador de reloj **1102** está configurado para generar un reloj de lanzamiento (para el LC LFSR 1104) y un reloj de captura (para el REBEL 1106). A continuación, en la FIG. D (graficada a partir de la FIG. 1 de D1) se identifica el controlador LC LFSR 1104 en color amarillo, el controlador REBEL 1106 en color verde, los vectores de lanzamiento aleatorio en color rojo, y el generador de reloj 1102 en color café:

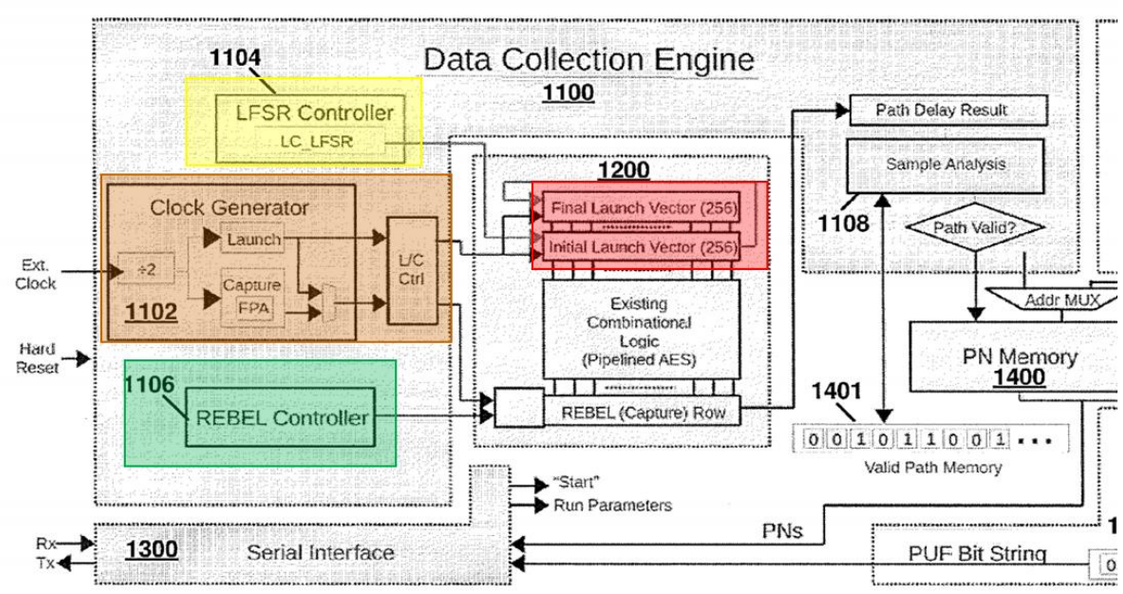

FIG. D

Adicionalmente, D1 divulga un motor de análisis de muestras (SAE) 1108 que analiza los resultados digitalizados en la cadena de retraso después de cada prueba de LC *(launch-capture)* para una ruta determinada y determina si la ruta es "válida". La memoria de ruta válida 1401 registra un indicador de aprobación / falla para cada ruta probada que refleje su validez. Los paquetes de números válidos (PN) se guardan en una memoria PN 1400. A continuación, en la FIG. E (graficada a partir de la FIG. 1 de D1) se identifica el motor de análisis de muestras (SAE) 1108 en color rosa, y la memoria PN 1400 en color azul claro:

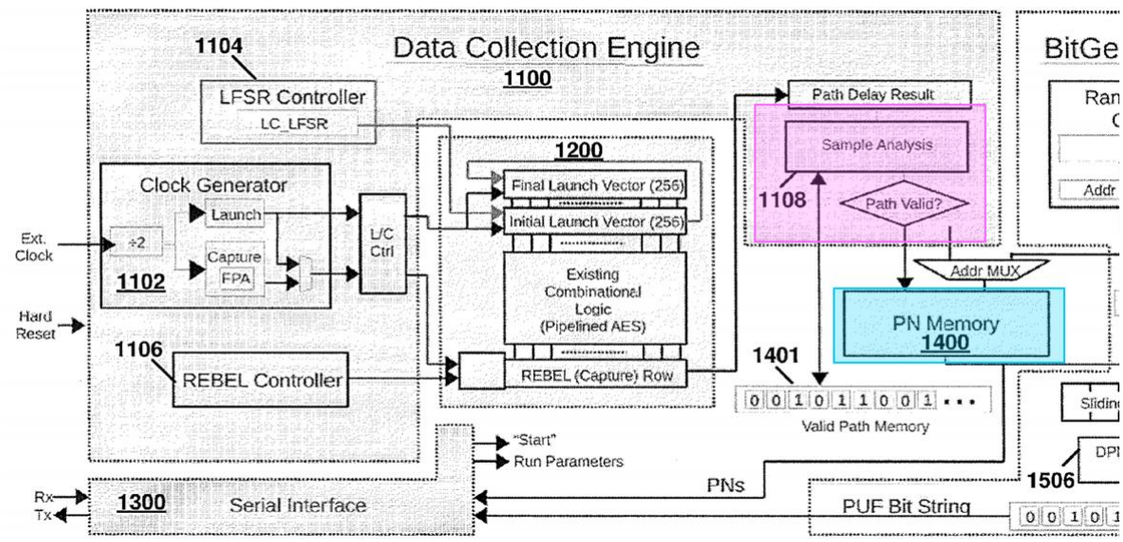

FIG. E

También, D1 menciona un motor de generación de bits 1500 que tiene un generador de emparejamiento aleatorio 1502 para generar emparejamientos aleatorios de (packet numbers) PN para la generación de bits; una memoria de punto de parada 1504, que registra

"puntos de parada" o "bits fuertes". Además, D1 divulga que puede usarse una técnica 'Dual-PN Count' (DPNC) 1506 que posprocesa los PNs para eliminar el sesgo. A continuación, en la FIG. F (graficada a partir de la FIG. 1 de D1) se identifica el motor de generación de bits 1500 en color amarillo, el generador de emparejamiento aleatorio 1502 en color verde claro, la memoria de punto de parada 1504 en color morado y el módulo que ejecuta la una técnica 'Dual-PN Count' (DPNC) 1506 en color gris:

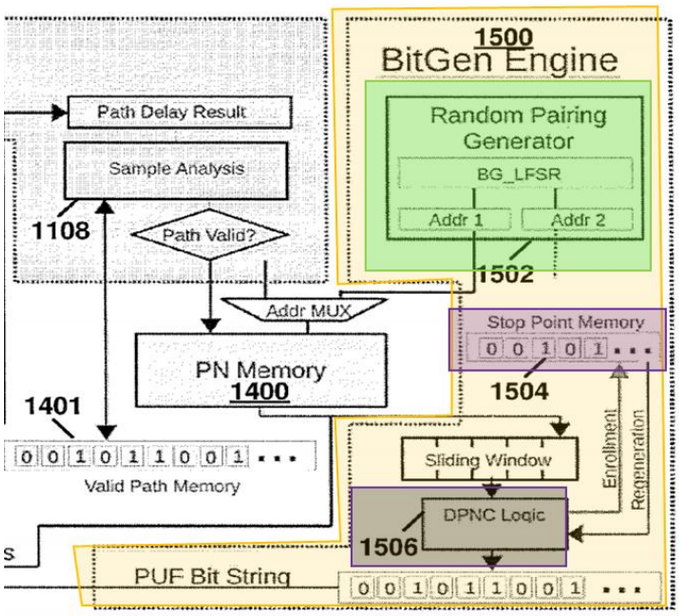

FIG. F

iii) Ahora bien, me permito respetuosamente señalar que la presente invención no se relaciona con dispositivos para la generación de funciones físicamente no clonables, las cuales se usan por lo general para formar seriales de chips. Por el contrario, la presente invención se relaciona con dispositivos tipo TRNG (**True Random** Number Generator, por sus siglas en inglés) los cuales están dirigidos a obtener números aleatorios o cadenas de números aleatorios, mas no PUFs.

En cuanto a las diferencias entre el arte previo citado por el Despacho y la nueva Reivindicación 1, me permito argumentar lo siguiente:

- D1 no divulga dos fuentes de entropía; y
- 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).

Por el contrario, D1 divulga que 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 fuente dual de entropía es un beneficio significativo para mejorar la aleatoriedad de las cadenas de bits no aleatorias generadas, así como para aumentar la dificultad de los ataques de ingeniería inversa. Sin embargo, D1 utiliza **una ÚNICA fuente de entropía**, de la cual saca dos componentes. Además, D1 divulga que **la semilla la proporciona un usuario** en el controlador LC LFSR 1104 para producir los vectores de lanzamiento aleatorio.

A continuación, se muestra en la FIG. G, en su lado izquierdo la FIG. 1 de D1, y en su lado derecho la FIG. 1 de la presente Solicitud de Patente. En la figura de D1 se muestra que **la semilla la proporciona un usuario** en el controlador LC LFSR, el cual es una unidad determinística en la cual se conoce su salida a partir de sus entradas (semilla). Por lo tanto, los vectores generados por el controlador LC LFSR son **número pseudoaleatorios**. En cambio, en la invención de la Reivindicación 1**, la semilla es tomada a partir de la segunda fuente de entropía,** la cual, al combinarse con la primera fuente entropía, genera que la unidad determinística de muestreo obtenga un **número aleatorio** (contario al número pseudoaleatorio del controlador LC LFSR de D1).

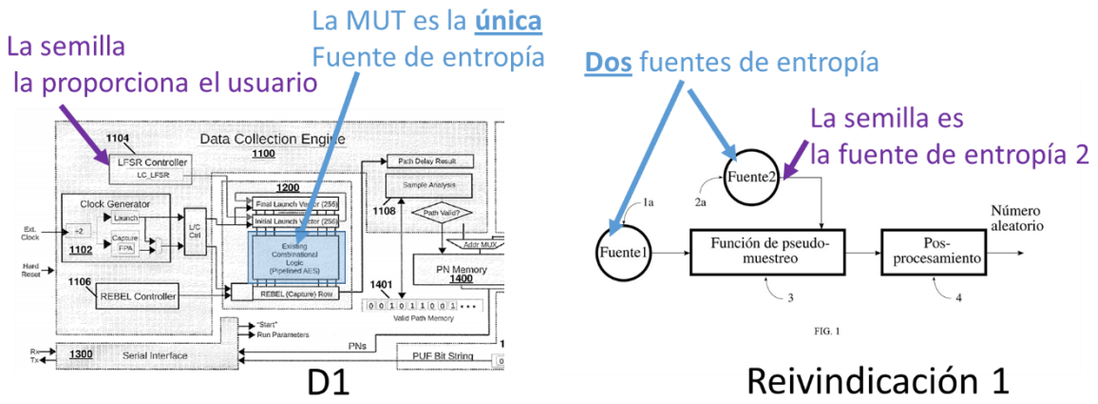

FIG. G

En consecuencia, el sistema divulgado por D1 ejecuta una serie de pasos que inician cuando un usuario suministra la semilla en el controlador LFSR 1104 para generar el par de vectores pseudoaleatorios. Estos vectores se suministran a la macro bajo prueba (MUT), la cual se usa como única fuente de entropía con dos componentes; estabilidad del camino y variaciones dentro del dado en el retraso. La macro bajo prueba (MUT) corre los vectores en dos caminos lógicos *"iguales"* que generan un desfase o retraso y una inestabilidad de

camino. Estos componentes son capturados y amplificados por el controlador REBEL 1106 mediante las cadenas de flip-flops. Los resultados de la captura y amplificación del retraso e inestabilidad en los caminos lógicos de la MUT son procesados en la unidad de análisis de muestras 1108 que determinan su validez. Los resultados válidos se alimentan al motor de generación de bits 1500, el cual genera la cadena de números pseudoaleatorios, y le aplica una técnica 'Dual-PN Count' (DPNC) 1506 que posprocesa los PNs para eliminar el sesgo.

Por el contrario, en la presente invención, el generador de números aleatorios obtiene números aleatorios (no pseudoaleatorios, como D1), a partir de la unidad determinística de muestreo (3) que se acopla en una de sus entradas a la primera fuente de entropía (1a) y usa como semilla la segunda fuente de entropía (2a). De esta manera, a partir de la combinación de fuentes de entropía que pueden tener algún tipo de sesgo, se obtiene un número completamente aleatorio sin sesgo, o con uno mínimo que se elimina por completo con la ayuda de la unidad determinística de posprocesamiento (4).

En consecuencia, en estructura y funcionalidad D1 es completamente diferente de la presente invención, por lo cual no podría afectar la novedad de la Reivindicación 1.

De acuerdo con lo anterior, con el fin de fundamentar una afectación válida contra la novedad de una invención, me permito señalar que, de acuerdo al MAP, el arte previo debe divulgar **explícitamente todas y cada una** de las características de la invención.[1] Es más, el Tribunal Andino de Justicia (TAJ) ha determinado que para establecer una objeción válida contra la novedad, la divulgación del arte previo debe ser lo suficientemente detallada para que una persona versada en la materia pueda usar dicha información para reproducir y explotar la invención.[2]. En el presente caso, nada en D1 anticipa completamente las características estructurales esenciales reclamadas en la presente invención por lo que resulta nueva frente al arte previo citado.

iv) Finalmente, en relación con la novedad de las Reivindicaciones 2 a 14, dichas Reivindicaciones incluyen todas las características novedosas de la Reivindicación 1, por lo cual también cumplen con el requisito de novedad.

[1] Manual Andino de Patentes, 2004, Sección 9.4
[2] Proceso 06-IP-89 (http://intranet.comunidadandina.org/Documentos/Procesos/209-IP-2005.doc); y Proceso 36-IP-2004 (http://www.notinet.com.co/serverfiles/servicios/archivos/30jul04/ca36-04.htm)

4. a- El Despacho indica que el título no se relaciona con el objeto de la solicitud, ni el contenido del Capítulo Descriptivo ni las reivindicaciones, por lo cual sugiere modificarlo.

b- Con el objetivo de facilitar el trámite de la presente solicitud, y siguiendo la amable sugerencia del Despacho, me permito indicar que se cambió el título de la presente invención de la siguiente manera:

"DISPOSITIVO GENERADOR DE CADENAS ALEATORIAS DE BITS USANDO FUENTES DE ENTROPÍA"

Por lo tanto, considero superada la anterior objeción.

5. 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

Anexo:
– Capítulo Reivindicatorio Modificado.