CAPÍTULO REIVINDICATORIO MODIFICADO
(Primer Examen de Fondo)

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).

****