(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 647 130**

(51) Int. CI.:

G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.07.2005 PCT/US2005/025610**

(87) Fecha y número de publicación internacional: **09.02.2006 WO06014656**

(96) Fecha de presentación y número de la solicitud europea: **18.07.2005 E 05774710 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.09.2017 EP 1774433**

(54) Título: **Procedimiento y aparato para generador de números aleatorios**

(30) Prioridad:

23.07.2004 US 897589

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.12.2017

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 MOREHOUSE DRIVE
SAN DIEGO, CALIFORNIA 92121, US

(72) Inventor/es:

SIMON, HARRIS S.;
VAN PELT, KENNETH ANDREW y
SHARP, DALE OGDEN

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Procedimiento y aparato para generador de números aleatorios

[0001] La presente invención se refiere a generadores de números aleatorios. Más específicamente, la presente invención se refiere a procedimientos y aparatos para generadores de números aleatorios estables, consistentes y auto-calibrados para la producción de gran volumen de dispositivos de comunicación inalámbrica.

ANTECEDENTES

[0002] En terminales o dispositivos de comunicaciones inalámbricas, existe una necesidad de generadores de números aleatorios, por ej., para aplicaciones criptográficas. Sin embargo, variaciones en las condiciones de funcionamiento (tales como cambios de temperatura, tensión y corriente) y variaciones en las características de los componentes (debido a inconsistencias en la fabricación de los componentes, envejecimiento, tiempo de conservación y vida útil) hacen que los generadores de números aleatorios existentes varíen en rendimiento a la hora de generar números aleatorios. En consecuencia, dispositivos similares fabricados para actuar de manera uniforme fluctúan en su rendimiento porque los generadores de números aleatorios constitutivos varían en sus características y, de este modo, producen diferentes distribuciones de números aleatorios.

[0003] Un dispositivo de este tipo se divulga en la solicitud de patente de Estados Unidos US-A-4 853 884 que se enfrenta al problema de un patrón de distribución estadística sesgado resultante (más 1s que 0s, o viceversa) causado por diferencias entre diferentes fuentes y condiciones ambientales. Las publicaciones EP-A-0 903 665 y "*A High Speed Truly IC Random Number Source for Smart Card Microcontrollers*" ("Una Fuente de Verdaderos Números Aleatorios de CI de Alta Velocidad para Microcontroladores de Tarjeta Inteligente" de BUCCI M et al se enfrentan a un problema similar. En EP-A-0903665, se obtiene un valor medio de una señal de números aleatorios y se usa para ajustar automáticamente una cantidad de desviación a cero.

[0004] Por lo tanto, existe una necesidad de que los generadores de números aleatorios rindan uniformemente a pesar de las variaciones en las características de los componentes, las condiciones de funcionamiento y el entorno. También existe una necesidad de que los dispositivos fabricados de forma similar funcionen de forma similar y muestren un rendimiento uniforme y constante.

RESUMEN

[0005] Los modos de realización divulgados proporcionan procedimientos y aparatos nuevos y mejorados para generar números aleatorios. En un aspecto, un procedimiento para generar números aleatorios para uso en un dispositivo de comunicación inalámbrica permite generar números aleatorios y recopilar una muestra de los números aleatorios generados. El procedimiento proporciona además el cálculo de al menos dos métricas que incluyen un valor medio y una desviación estándar, en base a la muestra recopilada, y comparando cada métrica con un valor de referencia correspondiente. El procedimiento proporciona además el ajuste de cada métrica en base a un resultado de la comparación de modo que los números aleatorios generados alcancen una distribución deseada.

[0006] En otro aspecto, un aparato para generar números aleatorios incluye un generador de ruido analógico y componentes de hardware para generar números aleatorios y valores de realimentación para ajustar los números aleatorios y su distribución. El aparato incluye además un procesador capaz de ejecutar instrucciones para llevar a cabo algoritmos de control para ajustar los números aleatorios y su distribución.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0007] Las características y ventajas de la presente invención resultarán más evidentes a partir de la descripción detallada de los modos de realización en relación con los dibujos que se exponen a continuación:

La FIG. 1 ilustra un diagrama de bloques de un generador de números aleatorios;
La FIG. 2 ilustra un diagrama de flujo para generar números aleatorios;
La FIG. 3 ilustra formas de onda de tensión de ruido para dispositivos fabricados de forma similar;
La FIG. 4 ilustra distribuciones de números aleatorios para dispositivos fabricados de forma similar sin ajuste; y
La FIG. 5 ilustra distribuciones similares de números aleatorios para dispositivos fabricados de forma similar con ajuste automático.

DESCRIPCIÓN DETALLADA

[0008] Antes de que se expliquen en detalle varios modos de realización, debe entenderse que el alcance de la invención no debe limitarse a los detalles de la construcción y la disposición de los componentes expuestos en la siguiente descripción o ilustrados en los dibujos. Además, debe entenderse que la fraseología y la terminología utilizadas en el presente documento son para fines de descripción y no deben considerarse limitantes.

[0009] La FIG. 1 ilustra un diagrama de bloques de un generador de números aleatorios con auto-ajuste automático 100, de acuerdo con un modo de realización. El generador de números aleatorios 100 incluye en general hardware de generador de ruido analógico 102, hardware de procesador de control 104 y módulo de software de procesador de control 106. El hardware de generador de ruido analógico 102 proporciona una tensión analógica aleatoria que se distribuye normalmente con un valor medio X y una desviación estándar S. El hardware del generador de ruido analógico 102 puede incluir también un diodo de ruido 108 y un amplificador 110 para acondicionamiento de señal, de acuerdo con un modo de realización. El diodo de ruido puede usarse en su región de descompresión inversa, predispuesta para funcionar sobre el "codo" de esta parte de la característica de funcionamiento. Cuando el diodo se acciona en esta región, la tensión de CA en sus terminales es una distribución gaussiana con una densidad espectral plana sobre su ancho de banda.

[0010] El hardware del procesador de control 104 incluye un ADC (convertidor de analógico a digital) 112, una CPU (unidad de procesamiento central) u ordenador y DAC (convertidores de digital a analógico) 114 y 116. El ADC 112 cuantifica la tensión de ruido analógica normalmente distribuida en base al valor de referencia de tensión (V-Ref) y genera números aleatorios. La CPU junto con el módulo de software de control calcula al menos una métrica, en base a una muestra de la tensión de ruido cuantificada, por ej. números aleatorios, ajusta la entrada de tensión de referencia (V-Ref) al ADC 112 y la entrada de desviación de CC del amplificador 110, con el fin de "ajustar" la distribución de los números aleatorios en la "ventana" de gama completa de la capacidad del ADC. La desviación de CC representa la media X de los números aleatorios, y la tensión de referencia (V-Ref) representa la desviación estándar de los números aleatorios. La tensión de referencia del ADC corresponde a la capacidad de cuantificación a escala completa del ADC, es decir, establece la tensión máxima en el ADC que puede digitalizarse sin sobrecargar el convertidor. Por lo tanto, ajustar la tensión de referencia es directamente proporcional a la conversión de tensión pico a pico del ADC.

[0011] De acuerdo con un modo de realización, el módulo de software del procesador de control 106 funciona sobre una muestra de números aleatorios producidos por el ADC 112 y calcula la media X y la desviación estándar S de la muestra elegida para devolvérselos a los DAC 114 y 116, respectivamente. El valor medio X se usa para controlar la localización del pico del histograma de los números aleatorios generados por el ADC 112, como se muestra en la forma de onda 118. La desviación estándar S se utiliza para controlar el ancho del histograma de los números aleatorios generados por el ADC 112, como se muestra en la forma de onda 120.

[0012] En sistemas típicos de generadores de números aleatorios, donde sólo se construyen unos cuantos y el entorno de funcionamiento es cuasiestático, los sistemas pueden ajustarse cambiando sus partes para lograr una distribución consistente de números aleatorios en todos los sistemas. Sin embargo, en una producción de gran volumen, como los teléfonos móviles, existe una necesidad de capacidad de ajuste automático que proporcione una distribución consistente de números aleatorios a través de una producción de alto volumen y bajo condiciones de funcionamiento variables.

[0013] La FIG. 2 ilustra un diagrama de flujo para ajustar distribuciones de números aleatorios, de acuerdo con un modo de realización. En la etapa 202, se eligen algunos valores iniciales para la desviación de CC y la tensión de referencia (V-Ref), que pueden ser los valores finales obtenidos cuando se ajustó por última vez el generador de números aleatorios. En la etapa 204, se selecciona una muestra de los números aleatorios producidos por el ADC 112. En la etapa 206, se calcula el valor medio de la muestra seleccionada de números aleatorios y se compara con un valor medio de referencia. El valor medio de referencia puede elegirse en base al ancho de bit ADC del generador de números aleatorios. Por ejemplo, para un ADC de 8 bits, la referencia o el valor medio deseado sería 127 para ajustarse a un histograma de números aleatorios gaussianos deseado 122. El valor medio de referencia de 127 corresponde al punto medio de la gama ADC de 8 bits. En base a la comparación llevada a cabo en la etapa 206, la entrada de valor de desviación de CC al amplificador 110 se ajusta, en la etapa 208 ó 210, según sea el caso, a través de algún algoritmo de control lineal, no lineal o adaptativo bien conocido en la técnica.

[0014] De forma similar, en la etapa 212, se calcula el valor de desviación estándar de la muestra seleccionada de números aleatorios y se compara con un valor de desviación estándar de referencia. El valor de desviación estándar de referencia puede elegirse en base a la precisión o el valor de escala completa de ADC del generador de números aleatorios. Por ejemplo, para un ADC de 8 bits 112, el valor de referencia o de desviación estándar deseada sería aproximadamente 42 para adaptarse al histograma de números aleatorios gaussianos deseado 122. El valor de desviación estándar de referencia de 42 corresponde a aproximadamente una sexta parte del rango de ADC de 8 bits, proporcionando una distribución de números aleatorios de seis sigma en el ADC. Basándose en la comparación realizada en la etapa 212, la entrada al DAC 116 se ajusta, en la etapa 214 ó 216, según sea el caso, a través de algún algoritmo de control lineal, no lineal o adaptativo bien conocido en la técnica.

[0015] La FIG. 3 ilustra tres formas de onda de tensión de ruido generadas por tres dispositivos fabricados de forma similar. Estas formas de onda de tensiones de ruido corresponden a las señales generadas en la salida de los respectivos amplificadores 110. Estas formas de onda en general tienen diferentes valores de desviación media y estándar, debido a la diferencia en las características del componente constituyente, las condiciones de funcionamiento, y el entorno.

[0016] La FIG. 4 ilustra tres distribuciones de números aleatorios para los tres dispositivos fabricados de forma similar mencionados anteriormente en relación con la FIG. 3, sin ajuste automático. Estas distribuciones de números aleatorios corresponden a los números aleatorios generados en la salida de los respectivos ADC 112. Siguen teniendo diferentes valores de desviación media y estándar.

[0017] La FIG. 5, sin embargo, ilustra tres distribuciones uniformes de números aleatorios para los dispositivos fabricados de forma similar mencionados anteriormente en relación con la FIG. 3, con mecanismo de ajuste automático. Estas distribuciones de números aleatorios corresponden a los números aleatorios generados en la salida de los respectivos ADC 112. Deseablemente tienen valores de desviación media y estándar iguales o muy cercanos, a pesar de la diferencia en las características de sus componentes constituyentes, condiciones de funcionamiento y entorno.

[0018] Por lo tanto, el procesador de control y el módulo de software divulgados en el presente documento ajustan el generador de números aleatorios para producir distribuciones de números aleatorios similares a través de numerosos dispositivos fabricados de forma similar bajo condiciones de funcionamiento variables. Por ejemplo, después de haber cumplido los criterios de ajuste de sigma y media, el generador de números aleatorios se considera calibrado y listo para proporcionar números aleatorios para la aplicación deseada con métricas que son consistentes con la producción inicial, las variaciones ambientales y el ciclo de vida del producto.

[0019] En otro modo de realización, se pueden calcular y ajustar también métricas adicionales tales como entropía, que indica cuánta aleatoriedad existe en los números aleatorios generados, para ajustar el rendimiento del generador de números aleatorios.

[0020] Los expertos en la técnica entenderán que la información y las señales pueden representarse usando cualquiera de entre varias tecnologías y protocolos diferentes. Por ejemplo, los datos, las instrucciones, las órdenes, la información, las señales, los bits, los símbolos y los segmentos que puedan haber sido mencionados a lo largo de la descripción anterior pueden representarse mediante tensiones, corrientes, ondas electromagnéticas, campos o partículas magnéticos, campos o partículas ópticos, o cualquier combinación de los mismos.

[0021] Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativos, en general, en lo que respecta a su funcionalidad. Que dicha funcionalidad se implemente como hardware o software depende de la aplicación específica y de las restricciones de diseño impuestas al sistema completo. Los expertos en la técnica pueden implementar la funcionalidad descrita de formas distintas para cada aplicación particular, pero no debe interpretarse que dichas decisiones de implementación supongan una desviación del alcance de la presente invención, que está definido por las reivindicaciones adjuntas.

[0022] Los diversos bloques lógicos, módulos y circuitos ilustrativos descritos en relación con los modos de realización divulgados en el presente documento pueden implementarse o realizarse con un procesador de propósito general, con un procesador de señales digitales (DSP), con un circuito integrado de aplicación específica (ASIC), con una matriz de puertas de campo programable (FPGA) o con otro dispositivo de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos, o con cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador pero, de forma alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un procesador también puede implementarse como una combinación de dispositivos informáticos, por ej., una combinación de un DSP y un microprocesador, una pluralidad de microprocesadores, uno o más microprocesadores conjuntamente con un núcleo de DSP o cualquier otra configuración de este tipo.

[0023] Las etapas de un procedimiento o algoritmo descrito en relación con los modos de realización divulgados en el presente documento pueden realizarse directamente en hardware, en un módulo de software ejecutado por un procesador o en una combinación de los dos. Un módulo de software puede residir en una memoria RAM, una memoria flash, una memoria ROM, una memoria EPROM, una memoria EEPROM, registros, un disco duro, un disco extraíble, un MSROM o en cualquier otra forma de medio de almacenamiento conocido en la técnica. Un medio de almacenamiento a modo de ejemplo está conectado al procesador de tal manera que el procesador puede leer información de, y escribir información en, el medio de almacenamiento. De forma alternativa, el medio de almacenamiento puede estar integrado en el procesador. El procesador y el medio de almacenamiento pueden residir en un ASIC. El ASIC puede residir en un terminal de usuario. De forma alternativa, el procesador y el medio de almacenamiento pueden residir como componentes discretos en un terminal de usuario.

[0024] La descripción de los modos de realización divulgados se proporciona para permitir que cualquier experto en la técnica realice o use la presente invención. Diversas modificaciones de estos modos de realización pueden

resultar fácilmente evidentes a los expertos en la técnica, y los principios genéricos definidos en el presente documento pueden aplicarse a otros modos de realización, por ej. en un servicio de mensajería instantánea o cualquier aplicación de comunicación de datos inalámbrica general, sin apartarse del espíritu o el alcance de la invención. Por lo tanto, la presente invención no pretende limitarse a los modos de realización mostrados en el presente documento.

REIVINDICACIONES

1. Un procedimiento para generar números aleatorios para su uso en un dispositivo de comunicación inalámbrica, generándose los números aleatorios en un generador de números aleatorios (100) que comprende un generador de ruido analógico (102) que incluye un amplificador (110) que proporciona una tensión de ruido analógica y un convertidor de analógico a digital (112) adaptado para generar los números aleatorios a partir de la tensión analógica, el procedimiento comprendiendo:

generar (202) números aleatorios;
recopilar (204) una muestra de los números aleatorios generados;
calcular (206, 212) al menos un valor medio y un valor de desviación estándar en base a la muestra;
comparar (206, 212) los valores calculados con los valores de referencia correspondientes; y
ajustar automáticamente (208, 210, 214, 216) el generador de números aleatorios en base a un resultado de dicha comparación de manera que los números aleatorios generados alcancen una distribución deseada, el ajuste automático comprendiendo ajustar (208, 210) un valor de desviación de CC del amplificador en base a la comparación de la media, y ajustar (214, 216) un valor de tensión de referencia del convertidor de analógico a digital en base a la comparación de desviación estándar.

2. El procedimiento de la reivindicación 1, que comprende además calcular un valor de entropía basado en la muestra.

3. El procedimiento de la reivindicación 1, en el que el valor de entrada ajustable se ajusta (208, 210, 214, 216) a través de un algoritmo lineal.

4. El procedimiento de la reivindicación 1, en el que el valor de entrada ajustable se ajusta (208, 210, 214, 216) a través de un algoritmo no lineal.

5. El procedimiento de la reivindicación 1, en el que el valor de entrada ajustable se ajusta (208, 210, 214, 216) a través de un algoritmo adaptativo.

6. El procedimiento de la reivindicación 1, en el que la distribución deseada es una distribución gaussiana.

7. Un aparato para generar números aleatorios para uso en un dispositivo de comunicación inalámbrica, generándose los números aleatorios en un generador de números aleatorios (100) que comprende un generador de ruido analógico (102) que incluye un amplificador (110) que proporciona una tensión de ruido analógica y un convertidor de analógico a digital (112) adaptado para generar los números aleatorios a partir de la tensión analógica, el aparato comprendiendo:

medios (100) para generar (202) números aleatorios;
recopilar (204) una muestra de los números aleatorios generados;
medios (106) para calcular (206, 212) al menos un valor medio y un valor de desviación estándar basado en la muestra;
medios (106) para comparar (206, 212) los valores calculados con los correspondientes valores de referencia; y
medios (104, 106) para ajustar automáticamente (208, 210, 214, 216) el generador de números aleatorios en base a un resultado de dicha comparación de manera que los números aleatorios generados alcancen una distribución deseada, los medios para el ajuste automático comprendiendo medios (114, 118) para ajustar (208, 210) un valor de desviación de CC del amplificador en base a la comparación de media, y medios (116, 120) para ajustar (214, 216) un valor de tensión de referencia del convertidor de analógico a digital en base a la comparación de desviación estándar.

8. El aparato de la reivindicación 7, que comprende además medios para calcular un valor de entropía basado en la muestra.

9. El aparato de la reivindicación 7, en el que dichos medios para ajustar (104, 106) están adaptados para ajustar el valor de entrada ajustable a través de un algoritmo lineal.

10. El aparato de la reivindicación 7, en el que dichos medios para ajustar (104, 106) están adaptados para ajustar el valor de entrada ajustable a través de un algoritmo no lineal.

11. El aparato de la reivindicación 7, en el que dichos medios para ajustar (104, 106) están adaptados para ajustar el valor de entrada ajustable a través de un algoritmo adaptativo.

12. El aparato de la reivindicación 7, en el que la distribución deseada (122) es una distribución gaussiana.

13. Un medio legible por ordenador que representa medios adaptados para implementar un procedimiento para

generar números aleatorios en un dispositivo de comunicación inalámbrica de acuerdo con una cualquiera de las reivindicaciones 1 a 6 cuando se ejecuta en un ordenador.

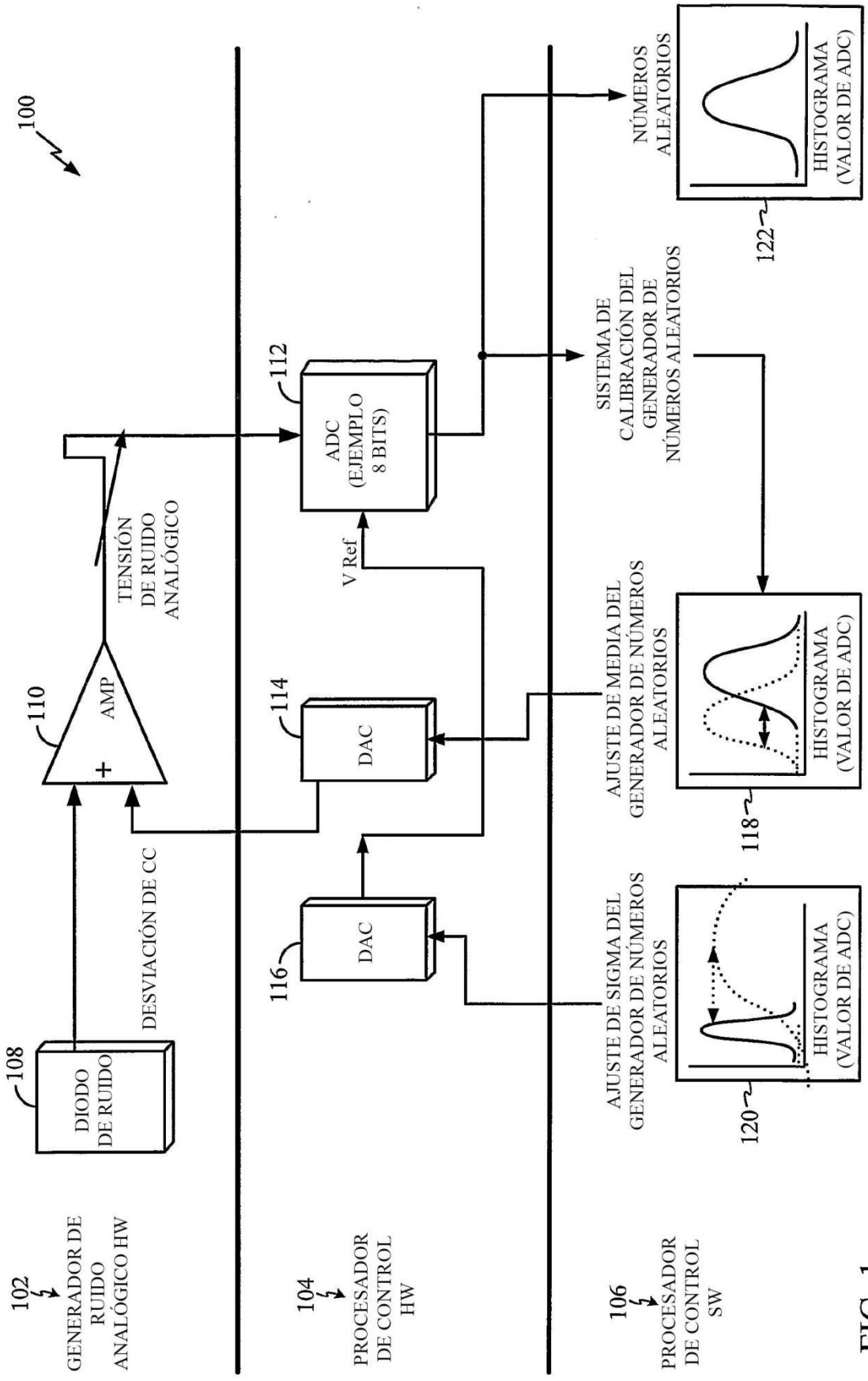
100
102
GENERADOR DE RUIDO ANALÓGICO HW
104
PROCESADOR DE CONTROL HW
106
PROCESADOR DE CONTROL SW
108
DIODO DE RUIDO
DESVIACIÓN DE CC
110
AMP
+
TENSIÓN DE RUIDO ANALÓGICO
112
ADC (EJEMPLO 8 BITS)
V Ref
114
DAC
116
DAC
AJUSTE DE SIGMA DEL GENERADOR DE NÚMEROS ALEATORIOS
AJUSTE DE MEDIA DEL GENERADOR DE NÚMEROS ALEATORIOS
SISTEMA DE CALIBRACIÓN DEL GENERADOR DE NÚMEROS ALEATORIOS
NÚMEROS ALEATORIOS
120
HISTOGRAMA (VALOR DE ADC)
118
HISTOGRAMA (VALOR DE ADC)
122
HISTOGRAMA (VALOR DE ADC)

FIG. 1

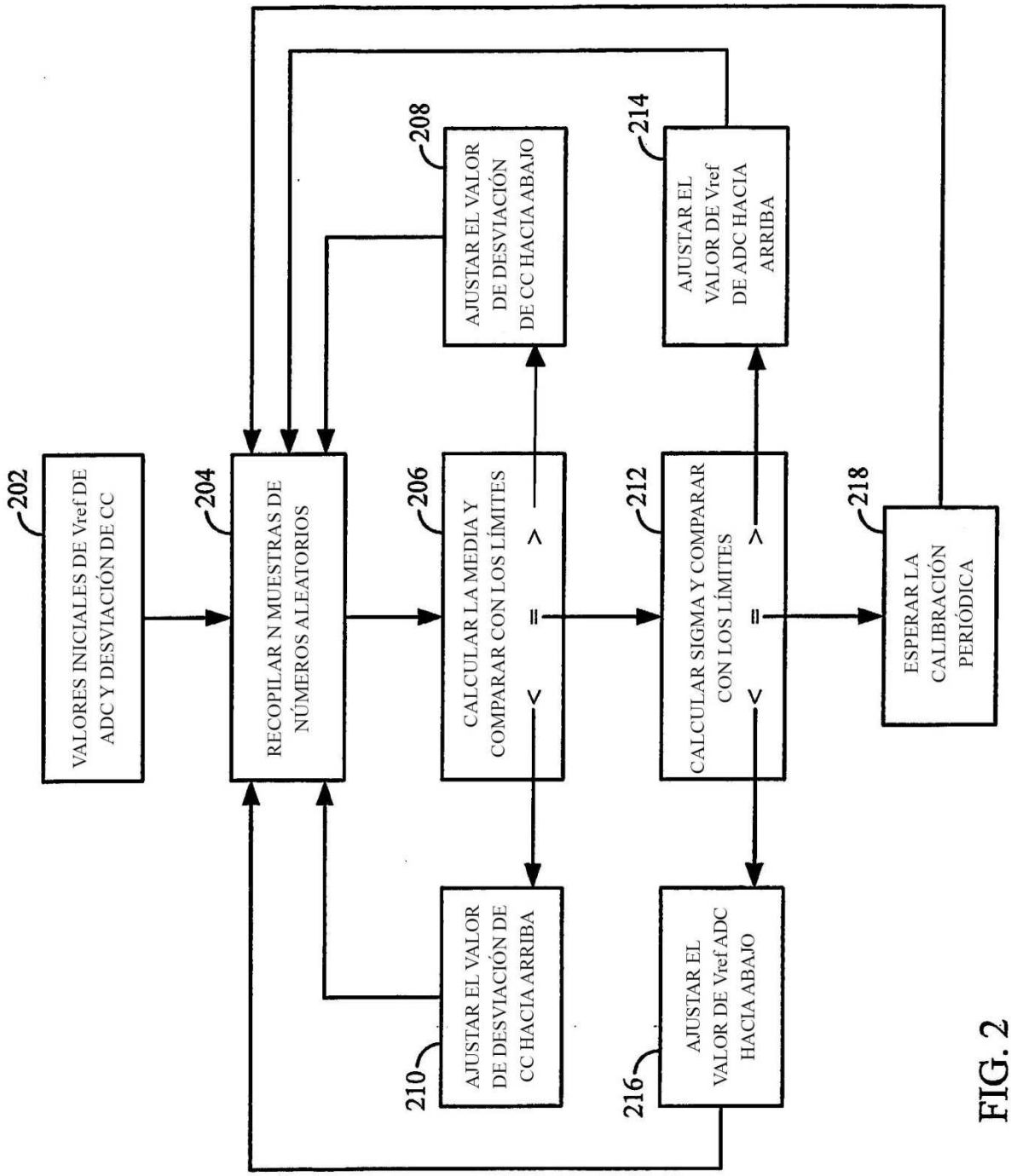
202
VALORES INICIALES DE Vref DE ADC Y DESVIACIÓN DE CC
204
RECOPILAR N MUESTRAS DE NÚMEROS ALEATORIOS
206
CALCULAR LA MEDIA Y COMPARAR CON LOS LÍMITES
>
=
<
208
AJUSTAR EL VALOR DE DESVIACIÓN DE CC HACIA ABAJO
210
AJUSTAR EL VALOR DE DESVIACIÓN DE CC HACIA ARRIBA
212
CALCULAR SIGMA Y COMPARAR CON LOS LÍMITES
>
=
<
214
AJUSTAR EL VALOR DE Vref DE ADC HACIA ARRIBA
216
AJUSTAR EL VALOR DE Vref ADC HACIA ABAJO
218
ESPERAR LA CALIBRACIÓN PERIÓDICA

FIG. 2

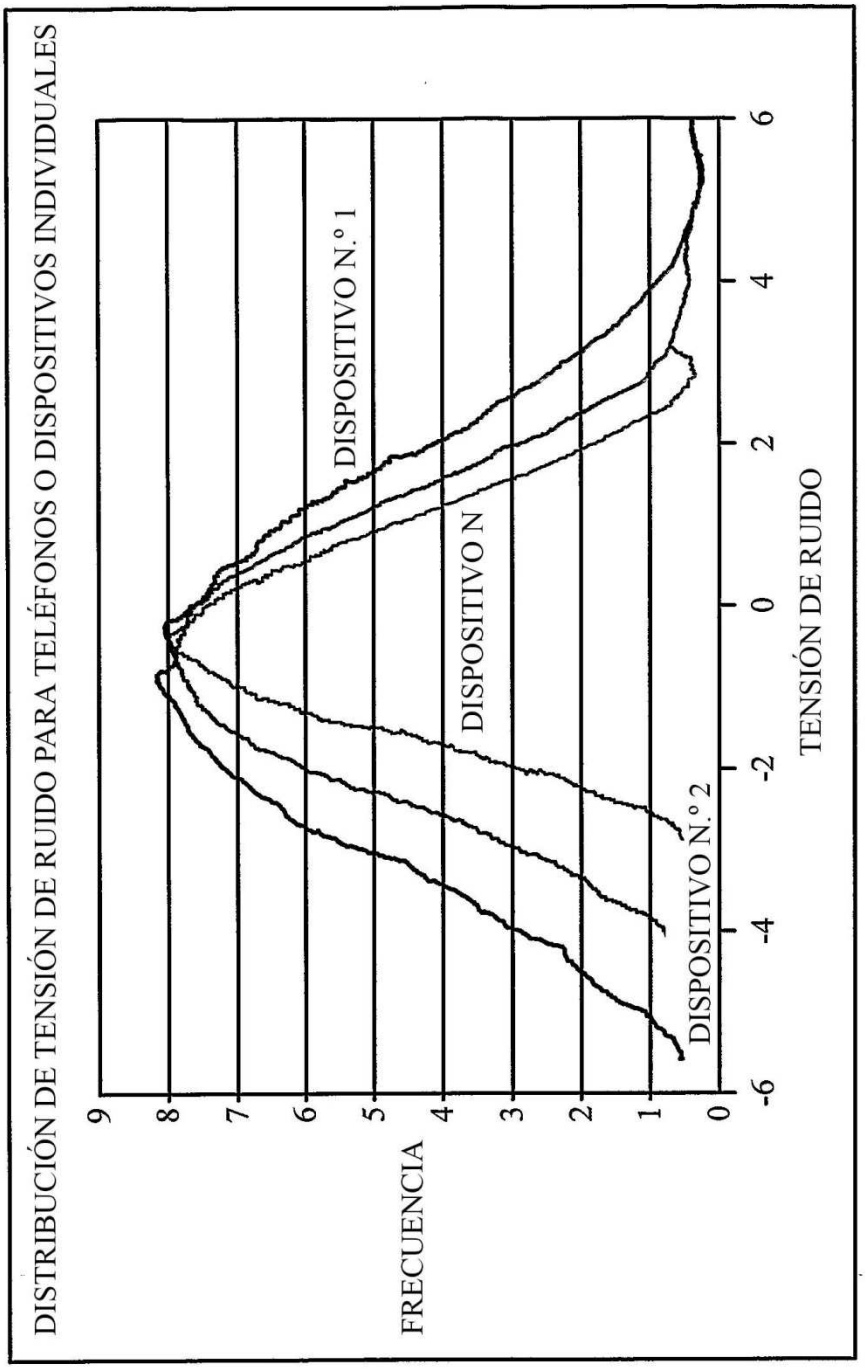
DISTRIBUCIÓN DE TENSIÓN DE RUIDO PARA TELÉFONOS O DISPOSITIVOS INDIVIDUALES
FRECUENCIA
TENSIÓN DE RUIDO
DISPOSITIVO N.º 1
DISPOSITIVO N
DISPOSITIVO N.º 2
9
8
7
6
5
4
3
2
1
0
-6
-4
-2
0
2
4
6

FIG. 3

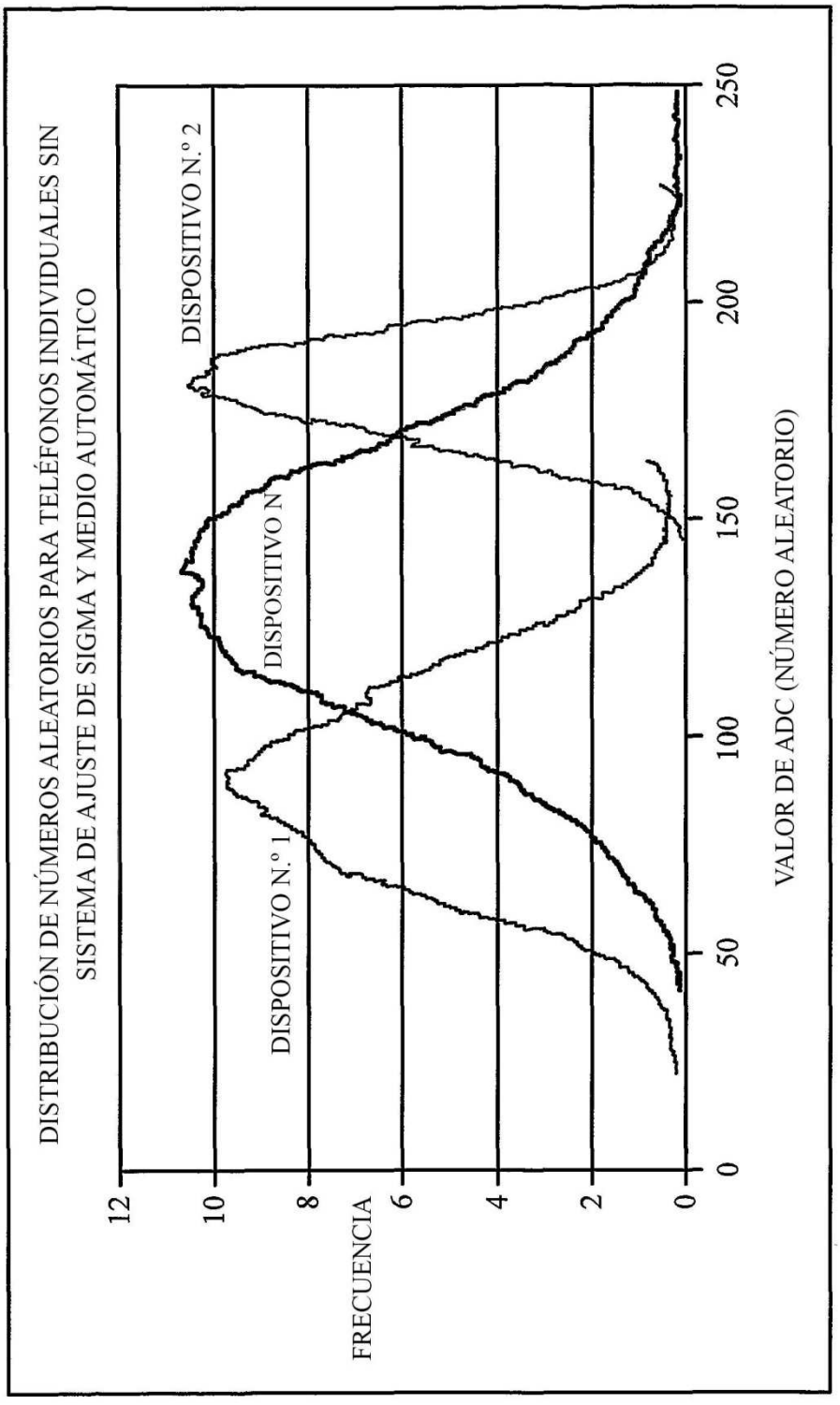
DISTRIBUCIÓN DE NÚMEROS ALEATORIOS PARA TELÉFONOS INDIVIDUALES SIN SISTEMA DE AJUSTE DE SIGMA Y MEDIO AUTOMÁTICO
DISPOSITIVO N.º 2
DISPOSITIVO N
DISPOSITIVO N.º 1
FRECUENCIA
12
10
8
6
4
2
0
0
50
100
150
200
250
VALOR DE ADC (NÚMERO ALEATORIO)

FIG. 4

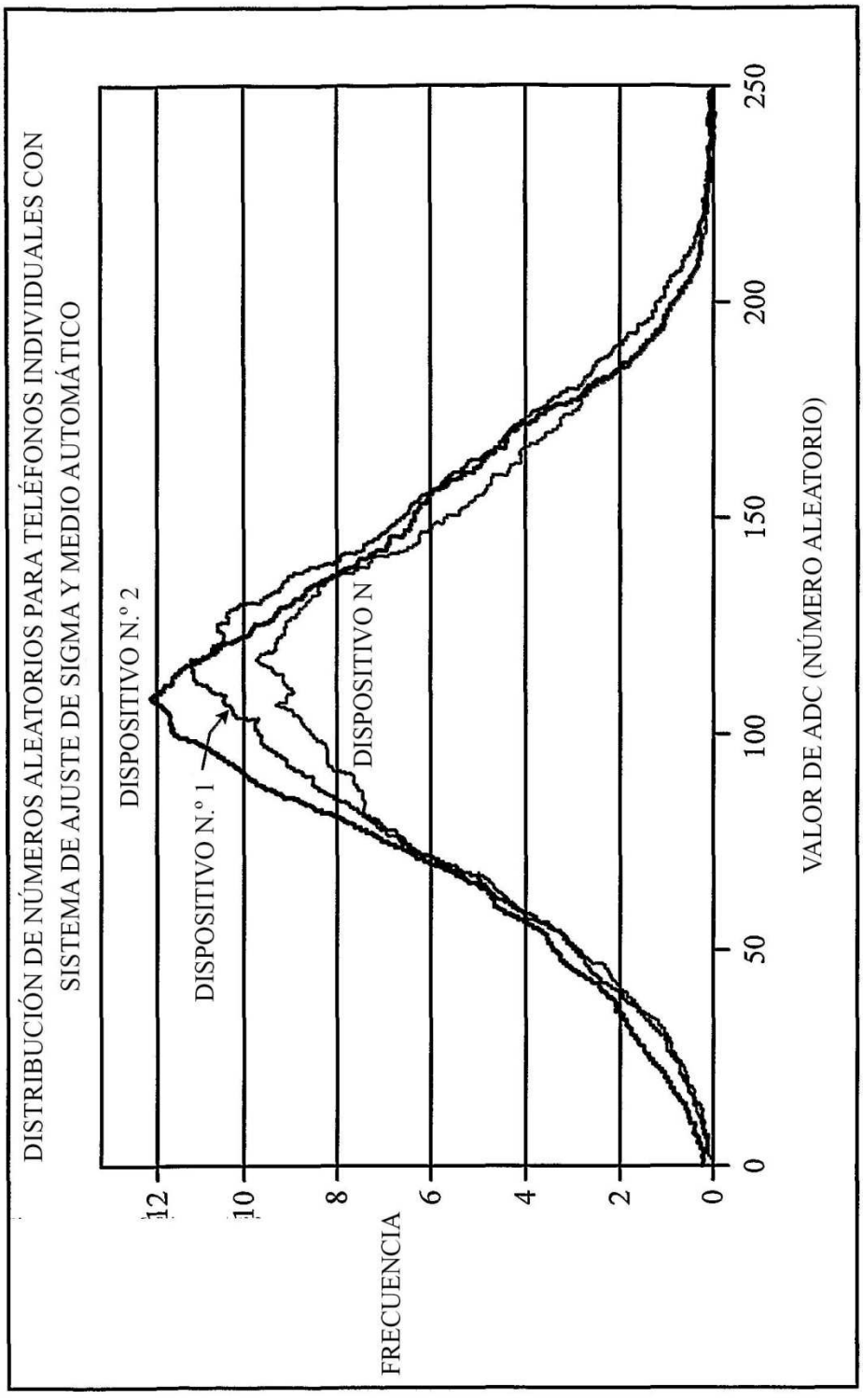
DISTRIBUCIÓN DE NÚMEROS ALEATORIOS PARA TELÉFONOS INDIVIDUALES CON SISTEMA DE AJUSTE DE SIGMA Y MEDIO AUTOMÁTICO
DISPOSITIVO N.º 2
DISPOSITIVO N.º 1
DISPOSITIVO N
FRECUENCIA
0
2
4
6
8
10
12
0
50
100
150
200
250
VALOR DE ADC (NÚMERO ALEATORIO)

FIG. 5