(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 686**

(51) Int. CI.:

G06F 7/58 (2006.01)
H04L 9/08 (2006.01)
H03K 3/84 (2006.01)
H04L 9/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.02.2014 PCT/EP2014/053819**

(87) Fecha y número de publicación internacional: **06.11.2014 WO2014177300**

(96) Fecha de presentación y número de la solicitud europea: **27.02.2014 E 14707725 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.02.2017 EP 2976707**

(54) Título: **Equipo y procedimiento para generar bits aleatorios**

(30) Prioridad:

03.05.2013 DE 102013208152

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2017

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

DICHTL, MARKUS

(74) Agente/Representante:

LOZANO GANDIA, José

EQUIPO Y PROCEDIMIENTO PARA GENERAR BITS ALEATORIOS

DESCRIPCIÓN

La presente invención se refiere a un equipo y a un procedimiento para generar uno o varios bits aleatorios. Se genera por ejemplo una secuencia de bits aleatorios, que se utiliza como número binario aleatorio. Los equipos y procedimientos propuestos para generar bits aleatorios sirven por ejemplo para implementar generadores de números aleatorios.

En aplicaciones relevantes para la seguridad, por ejemplo en procedimientos de autentificación asimétricos, son necesarias secuencias de bits aleatorios como números binarios aleatorios. Al respecto se desea, en particular en aplicaciones móviles, una inversión en hardware lo más reducida posible. Las medidas conocidas para generar números aleatorios son por ejemplo números pseudoaleatorios, fuentes aleatorias analógicas, osciladores en anillo y sus variantes.

En números pseudoaleatorios se utilizan seeds (valores iniciales o semillas), partiendo de los cuales se calculan números pseudoaleatorios deterministas. Para generar los seeds se utiliza por lo general un generador aleatorio físico. Como fuentes aleatorias analógicas se utilizan fuentes de ruidos, como por ejemplo el ruido de diodos Zener, amplificado y digitalizado. Al respecto el enlace entre las técnicas de conexión digital y analógica por lo general sólo puede realizarse con elevados costes.

En osciladores en anillo, que están constituidos por un número impar de inversores conectados uno tras otro, resultan jitter (fluctuaciones de fase) aleatorias debidas a tiempos de propagación oscilantes de las señales a través de los inversores. Estos jitter, es decir, oscilaciones irregulares en el tiempo cuando se modifica el estado de las señales enviadas a través de los inversores, pueden acumularse cuando se realizan varias pasadas a través del circuito del oscilador en anillo, con lo que en definitiva resulta una señal analógica aleatoria. Un inconveniente en los osciladores en anillo es a menudo el largo tiempo necesario desde el inicio de la oscilación hasta que resulta una señal aleatoria útil debido a la acumulación de jitter. Por ello resultan la mayoría de las veces en osciladores en anillo bajas velocidades de generación de datos, que son inaceptables. Además es posible que las aportaciones de jitter que se suman se anulen por sí mismas, con lo que en promedio los cortos tiempos de propagación aleatorios en las puertas se compensen mediante largos tiempos de propagación aleatorios en las puertas.

Los osciladores el anillo de Fibonacci y Galois generan formas de señal aleatorias más rápidas que las de los osciladores en anillo clásicos. Desde luego se utilizan diversas puertas digitales como puertas XOR y NOT. Debido a ello pueden resultar, en particular cuando se trata de implementaciones sobre ASICs, grandes diferencias de velocidades de los tipos de puertas. A menudo existe el deseo de generar secuencias de bits aleatorios con la ayuda de FPGAs (Field Programmable Gate Arrays, baterías de puertas programables en campo). Desde luego pueden generarse también en estos módulos digitales, por ejemplo debido a oscilaciones de la temperatura ambiente, oscilaciones periódicas, que sólo tienen una reducida entropía o aleatoriedad en las señales.

La solicitud de patente europea EP 1 643 643 A1 da a conocer un generador de números aleatorios con dos osciladores en anillo, estando prevista una realimentación de una señal de paridad externa.

Por ello un objetivo de la presente invención consiste en proporcionar un equipo y/o un procedimiento mejorados para generar bits aleatorios.

En consecuencia, se propone un equipo para generar bits aleatorios que incluye varios equipos de representación, estando preparado el equipo de representación correspondiente para representar una cantidad n predeterminada de señales de entrada con ayuda de una representación combinatoria en una cantidad p predeterminada de señales de salida. Al respecto están encadenados los equipos de representación entre sí y está configurado al menos un bucle de realimentación. El bucle de realimentación está configurado en particular tal que una variación del estado de al menos una señal de salida de un equipo de representación elegido se lleva como una variación del estado de al menos una señal de entrada a otro equipo de representación.

Con preferencia no es el otro equipo de representación ningún equipo de representación directamente contiguo.

Al respecto existe en particular un bucle de realimentación cuando una variación de estado de al menos una señal de salida de realimentación de un determinado equipo de representación se lleva como una variación de estado de al menos una señal de entrada de otro equipo de representación tal que una o varias señales de salida del equipo de representación determinado se vea/n influida/s por la variación del estado de la señal de salida de realimentación.

Además está establecida una representación combinatoria tal que una variación de estado de una señal de entrada del correspondiente equipo de representación en promedio se reproduzca en más de una señal de salida del correspondiente equipo de representación.

La cantidad n de señales de entrada del correspondiente equipo de representación puede corresponderse con la cantidad p de señales de salida. No obstante, puede también pensarse en que n sea diferente de p, es decir, que con ayuda del correspondiente equipo de representación se reproduzcan los estados de las señales de entrada en

estados de señales de salida, siendo la cantidad de señales de salida menor o mayor que la cantidad de señales de entrada para el correspondiente equipo de representación.

Los equipos de representación pueden ser puertas lógicas o combinatorias, que en particular realizan una representación biyectiva de n señales de entrada en n señales de salida. Las señales de entrada oscilan entre niveles que pueden asociarse a estados lógicos, como bits 1 o high o bien 0 o low. Bajo una reproducción biyectiva se entiende una reproducción inequívoca entre los 2^n valores lógicos posibles de las señales de entrada y los 2^n valores lógicos de las señales de salida.

En este sentido resulta con ayuda de los equipos de representación en unas formas de realización del equipo, un oscilador en anillo de n pistas. Los equipos de representación pueden denominarse también nodos o puertas. La correspondiente representación combinatoria está realizada en particular tal que en promedio cuando tiene lugar una variación del estado de una señal de entrada tiene lugar un cambio de estado en más de una señal de salida. Esto da lugar a que el correspondiente jitter de la señal de entrada se reproduzca en varias señales de salida y por lo tanto se amplifique. Un jitter que se presente una sola vez en una señal, se copia con ayuda de los equipos de representación o bien de las reproducciones combinatorias allí implementadas en varias pistas de salida, con lo que los componentes del jitter apenas pueden compensarse.

Se puede hablar en cuanto al equipo también de un circuito oscilador en anillo multipista. Respecto a los osciladores en anillo clásicos de una sola pista, existe en particular la ventaja de que pueden tomarse valores de bits aleatorios con una mayor velocidad de datos. Por ejemplo puede derivarse una señal de bits aleatoria en una o varias de las rutas de datos que resultan en base a las n señales de entrada y/o salida.

Se puede decir que el equipo desarrolla "oscilaciones" o propaga cambios de señal en el circuito. Con preferencia depende al menos una de las señales de salida causalmente de sí misma, al realimentarse, realizándose la realimentación con ayuda de varias representaciones intercaladas.

En una forma de realización del equipo está realizada al menos una representación combinatoria tal que las señales de entrada se reproducen, sometiéndolas a un jitter y a una función lógica, en las señales de salida. Mediante la implementación en hardware de la representación combinatoria mediante los equipos de representación, pueden resultar jitters, es decir, oscilaciones en la evolución en el tiempo de flancos de señal. Este jitter se retransmite entonces y se acumula, al realizarse por completo la función lógica, es decir, la representación de la combinación de n señales de entrada o valores de bit en n señales de salida o valores de bit a lo largo de los ciclos y la realimentación de los equipos de representación.

Con preferencia no son, al menos algunas de las representaciones, representaciones combinatorias que aportan exclusivamente una permutación de las señales de entrada en las señales de salida. Una permutación de las señales de entrada existe en particular cuando las señales de salida se corresponden con las señales de entrada, o bien resultan simplemente de una modificación de la secuencia de las señales de entrada. En una permutación no resulta ninguna "multiplicación " del jitter.

En unas formas de realización del equipo para generar bits aleatorios, están preparados los equipos de representación tal que sus tiempos de propagación de la señal son iguales. Mediante tiempos de propagación de la señal lo más iguales posible, se reduce el riesgo de que las aportaciones de los jitter se puedan compensar mutuamente. Además se facilita una implementación al modo de ASICs o FPGAs. Por ejemplo están preparados los equipos de representación tal que todos los cambios de estado se realizan en las correspondientes salidas dentro de un intervalo de tolerancia de 100 ps y con preferencia dentro de 50 ps.

En unas formas de realización del equipo, incluye al menos un equipo de representación una tabla lookup o tabla de consulta para implementar la representación combinatoria. También es posible que todos los equipos de representación estén dotados de la correspondiente tabla lookup. Las tablas lookup pueden leerse fácilmente y exigen sólo un pequeño coste en hardware. A menudo están previstas en chips de lógica programable, como FPGAs, los campos correspondientes o ya tablas.

En unas formas de realización del equipo, pueden llenarse las tablas lookup con valores de bits aleatorios utilizando elementos aleatorios. Es posible por ejemplo generar las tablas lookup, que en función de un patrón de bits de entrada en las entradas de los equipos de representación, aportan en las salidas el correspondiente patrón de bits de salida, tal que se elija la reproducción representada por la tabla lookup aleatoriamente a partir de todas las (2^n) biyecciones de n señales lógicas en n señales lógicas. Con preferencia están implementadas en los equipos de representación en cada caso distintas representaciones combinatorias.

En unas formas de realización del equipo, constituyen los equipos de representación encadenados entre sí un circuito de oscilador en anillo de varias pistas.

Puede pensarse en que en el equipo existan varios ramales de realimentación de equipos de representación encadenados. Es posible por ejemplo interconectar varias cadenas individuales a diversas realimentaciones.

En unas formas de realización del equipo, está preparado el equipo tal que en particular cuando se realiza un acoplamiento por primera vez de señales de entrada, las señales de entrada están predeterminadas tal que el

equipo no se encuentra en un punto fijo. Por ejemplo pueden aplicarse niveles fijos claramente definidos a las entradas de uno de los equipos de representación, para arrancar a partir de un estado bien definido. A continuación resulta mediante la realimentación y la aplicación encadenada de las representaciones combinatorias en las señales, una señal de bits aleatorios con la anchura de n o de p bits.

El equipo está preparado con preferencia en particular tal que el mismo no presenta ningún punto fijo. Para ello se eligen e implementan las representaciones combinatorias tal que no existe ningún punto fijo.

Con preferencia la cantidad predeterminada n y p de señales de entrada y señales de salida respectivamente, es de al menos tres. En unas formas de realización, la anchura de bits o la cantidad n y p de señales predeterminadas de entrada y de salida respectivamente en los equipos de representación es de cuatro o más.

En unas formas de realización del equipo está previsto un dispositivo de exploración, para explorar una o varias señales de salida en salidas de un equipo de representación. El dispositivo de exploración puede también captar la correspondiente señal de entrada o de salida en distintos equipos de representación. La exploración se realiza por ejemplo controlada por impulsos periódicos o bien en otros instantes predeterminados y sirve para deducir un valor de bit H o L, que debido a que la señal aleatoria oscila fuertemente, presenta una elevada entropía o aleatoriedad.

En unas formas de realización incluye el dispositivo de exploración al menos un elemento de almacenamiento intermedio. El elemento de almacenamiento intermedio puede presentar un flip-flop, como por ejemplo un T-flip-flop o un equipo latch. También puede pensarse en uno o varios contadores para captar flancos de señal o cambio de estado de señales individuales. Un T-flip-flop es en particular adecuado para contar flancos de señal ascendente o descendente módulo 2.

El equipo de detección puede estar equipado tal que una señal de salida se explore en función de otra señal de salida. También puede pensarse por ejemplo que un flanco de señal active (trigger) o provoque la exploración de otra señal de salida.

En unas formas de realización, el equipo es parte de un equipo FPGA o de un equipo ASIC.

Se propone además un procedimiento para generar bits aleatorios en el que se realizan varias representaciones combinatorias encadenadas una tras otra. Al respecto reproduce cada representación combinatoria una cantidad n predeterminada de señales de entrada en una cantidad p predeterminada de señales de salida. Encadenando representaciones combinatorias se forma al menos un bucle de realimentación. Entonces se elige al menos una representación combinatoria tal que una variación de estado de una señal de entrada se represente mediante las representaciones combinatorias en promedio en más de una señal de salida. La correspondiente señal de entrada puede por ejemplo representar el valor de un bit.

Con preferencia se forma el acoplamiento, de los que al menos hay uno, tal que una variación de estado de al menos una señal de salida de una representación combinatoria elegida se lleva como una variación de estado de al menos una señal de entrada de otra representación combinatoria.

Las representaciones combinatorias pueden denominarse representaciones de n en p.

El procedimiento puede implementarse en particular mediante lenguajes de descripción adecuados, por ejemplo VHDL o Verilog, o en un equipo FPGA o ASIC. En el equipo FPGA o bien en el procedimiento están preparados los equipos de representación con preferencia tal que variaciones de estado en una señal de entrada de las n señales de entrada, en función de la representación combinatoria, provocan en el mismo instante un cambio de estado en una o varias de las p señales de salida, lo más simultáneamente posible.

Otras posibles implementaciones de la invención incluyen también combinaciones no citadas explícitamente de equipos o variantes del procedimiento antes descritos o que se describen en lo que sigue en relación con los ejemplos de realización. Al respecto añadirá o modificará el especialista también aspectos individuales como mejoras o complementos a la correspondiente forma básica de la invención.

Las características, particularidades y ventajas de esta invención antes descritas, así como la forma para alcanzarlas, quedarán más claras y se entenderán mejor en relación con la siguiente descripción de los ejemplos de ejecución que se describirán más en detalle en relación con los dibujos.

Al respecto muestran:

figura 1 una representación esquemática de un primer ejemplo de realización de un equipo para generar bits aleatorios;

figura 2 una representación esquemática de un segundo ejemplo de realización de un equipo para generar bits aleatorios;

figuras 3 - 6 evoluciones en el tiempo de señales de bits aleatorios generados según ejemplos de realización del procedimiento y del equipo para generar bits aleatorios y

figura 7 una representación esquemática de un tercer ejemplo de realización de un equipo para generar bits aleatorios.

En las figuras están dotados los elementos que tienen las mismas funciones de las mismas referencias, siempre que no se indique otra cosa.

La figura 1 muestra una representación esquemática de un primer ejemplo de realización de un equipo para generar bits aleatorios. El equipo 1 está constituido a modo de un oscilador en anillo de n canales o n pistas. Para ello están acoplados en serie uno tras otro circuitos digitales combinatorios 2_1 a 2_m. Los circuitos digitales combinatorios 2_1 a 2_m pueden entenderse también como puertas lógicas o equipos de representación para la correspondiente representación combinatoria.

Cada equipo de representación 2_i tiene n entradas para una señal de entrada E_{ij} de n bits de anchura con j = 1...n y p salidas para una señal de salida de p bits de anchura A_{ij} con j = 1...p. En la figura 1 no se indican explícitamente las entradas y salidas. Un equipo de representación correspondiente 2_i recibe por lo tanto E_{i1} bis E_{in} señales de entrada y emite A_{i1} bis A_{ip} señales de salida. La combinación entre señales de entrada y señales de salida se realiza mediante una representación combinatoria K_i. Se observa en la representación de la figura 1, en la que es n = p, que las representaciones combinatorias K_1 a K_m se realizan encadenadas una tras otra y el resultado de la representación o las señales de salida A_{m1} bis A_{mp} se conduce/n como señales de entrada E_{11} bis E_{1n} al primer equipo de representación 2_1. Por lo tanto resulta una realimentación como en un oscilador en anillo.

Para lograr una realimentación no han de llevarse necesariamente todas las señales de salida A_{m1} a A_{mp} como señales de entrada E_{11} a E_{1n} a un equipo de representación 2_1 encadenado en la dirección de avance del circuito de señales. Básicamente es suficiente elegir una única señal de salida A_{ij} y llevarla a un equipo de representación 2_k antepuesto en el circuito de señales o ruta de señales, siempre que un cambio de estado de la señal $E_{kl} \sim A_{ij}$ existente en la correspondiente entrada dé lugar en promedio a cambios de estado en más de una de las señales de salida A_{ko} (o=1...n). Cuanto más señales de salida se realimenten, tanto más fuertemente se amplifica un jitter existente con ayuda de las representaciones combinatorias K_1 - K_m y se copia en los n "canales". Los equipos de representación tampoco tienen que tener forzosamente la misma cantidad de entradas y salidas n, pero para simplificar se explicarán aquí ejemplos con la misma cantidad de señales de entrada y señales de salida.

Puesto que los equipos de representación 2_1 a 2_m configuran una topología con forma anular, puede dar lugar también un acoplamiento en el sentido de avance de señales de salida A_{m1} a A_{mn} a entradas de equipos de representación 2_1 a 2_m encadenados en el sentido de avance a que flancos de señal afectados por jitter se propaguen a través de los equipos de representación encadenados 2_1 a 2_m y entonces los jitter se amplifiquen y se multipliquen.

El correspondiente equipo de representación 2_i con la representación combinatoria K_i implementada puede denominarse también nodo, puerta o circuito digital combinatorio. Las representaciones combinatorias K_1 a K_m implementadas en los equipos de representación 2_1 a 2_m están elegidas tal que una variación del correspondiente bit de entrada (input) o bien del estado lógico de una señal de entrada E_{ij} en promedio dé lugar a variaciones en más de uno de los bits de salida (output) del correspondiente nodo o del correspondiente equipo de representación. Por lo tanto se acumulan y multiplican jitter que existen en las señales E_{11} a E_{mn} o bien A_{11} a A_{mn}, en el recorrido a través de los equipos de representación encadenados 2_1 a 2_m.

El correspondiente tiempo de propagación en un equipo de representación o bien una puerta lógica o combinatoria 2_i es esencialmente igual para todas las señales de entrada E_{i1} a E_{in}, con lo que en base a la representación combinatoria K_i implementada, el cambio de un estado lógico en una señal de entrada E_{ij} es esencialmente simultáneo a cambios lógicos en una o varias señales de salida A_{il} con l Є {1, 2,...n}. Por lo tanto resultan n canales con formas de señal aleatorias, provocadas por los jitter, que son provocadas por los elementos de conmutación que constituyen los equipos de representación digitales.

Se prevé un dispositivo de exploración 4, que por ejemplo capta una o varias de las señales de salida A_{m1} bis A_{mn} del equipo de representación 2_m y que, puesto que resulta en cada caso una forma aleatoria de evolución de la señal, deduce de ello una señal de bit aleatoria ZB. Por ejemplo puede tomarse y captarse, con control mediante impulsos periódicos o según necesidades, un nivel de señal e interpretarse el mismo como un valor de bit H o L o bien 1 ó 0.

Es posible al respecto situar el aparato o el generador de bits aleatorios 1 en un estado inicial en el que no exista ningún punto fijo. Esto se realiza por ejemplo recibiendo en toda la anchura de bits n por ejemplo las señales de entrada E_{11} a E_{1n} para el primer equipo de representación 2_1 en cada caso un nivel claramente definido. Además puede estar interrumpida transitoriamente la línea de realimentación entre el equipo de representación 2_m y el equipo de representación 2_1. A continuación se deja que transcurra libremente la oscilación, con lo que resultan formas de señal aleatorias en los n canales o circuitos en los que puede realizarse la toma.

En la figura 1 se indica opcionalmente que también puede implementarse otra ruta de realimentación 3 (representada en línea discontinua). Básicamente pueden realizarse también topologías de realimentación más complicadas, por ejemplo a modo de topologías de Galois o Fibonacci con equipos de representación de n pistas.

El equipo indicado esquemáticamente para generar bits aleatorios 1 puede realizarse en particular económicamente en equipos FPGA o ASIC. En comparación con osciladores en anillo clásicos monocanal, pueden generarse bits aleatorios con una mayor velocidad de datos, ya que en particular el jitter que favorece la aleatoriedad puede

multiplicarse potencialmente n veces con la ayuda de los varios canales. Debido a la gran cantidad de canales y representaciones, es improbable que las aportaciones de los jitter puedan compensarse entre sí. En este sentido puede realizarse un generador de números aleatorios con una elevada frecuencia de generación de bits aleatorios.

En la figura 2 se muestra otro ejemplo de realización de un equipo para generar bits aleatorios. Esencialmente se representan los mismos elementos que en la figura 1, pero se realiza el generador de bits aleatorios 10 con ayuda de un módulo FPGA. Se tienen m = 10 puertas combinatorias o equipos de representación 2_1 a 2_{10} encadenados entre sí en serie y realimentados. Las puertas combinatorias 2_1 a 2_{10} tienen en cada caso cuatro entradas y cuatro salidas, con lo que resulta un oscilador en anillo de cuatro canales o cuatro pistas. Las representaciones combinatorias realizadas mediante las puertas 2_1 a 2_{10} resultan de las tablas lookup 5_1 bis 5_{10}.

En la siguiente tabla se muestra una representación combinatoria K_q a modo de ejemplo, que representa n = 4 estados de entrada o señales de entrada E_{q1} - E_{q4} en p=4 estados de salida o señales de salida A_{q1} - A_{q4}. Para simplificar la representación se supone que las señales de entrada E_{q1} - E_{q4} y las señales de salida A_{q1} - A_{q4} representan estados lógicos 0 ó 1 y L ó H respectivamente, aún cuando mediante la “aleatorización” y fuerte sometimiento a jitter aleatorios, más bien no existe ningún nivel lógico claramente definido en el equipo implementado como hardware o como circuito para generar bits aleatorios.

E_{q4}	E_{q3}	E_{q2}	E_{q1}	A_{q4}	A_{q3}	A_{q2}	A_{q1}
0	0	0	0	0	1	0	0
0	0	0	1	1	0	0	1
0	0	1	0	0	0	1	1
0	0	1	1	1	1	1	0
0	1	0	0	1	1	1	1
0	1	0	1	0	0	0	1
0	1	1	0	1	0	0	0
0	1	1	1	0	1	1	1
1	0	0	0	1	0	1	1
1	0	0	1	0	1	1	0
1	0	1	0	1	1	0	0
1	0	1	1	0	1	0	1
1	1	0	0	0	0	1	0
1	1	0	1	1	1	0	1
1	1	1	0	0	0	0	0
1	1	1	1	1	0	1	0

La tabla puede implementarse como tabla lookup para configurar el equipo de representación 2_q. Entonces se realiza una representación biyectiva, con lo que cualquier patrón de bits posible formado por cuatro bits de entrada o estados de señales de entrada E_{q1}, E_{q2}, E_{q3}, E_{q4} se presenta exactamente una vez en las salidas del equipo de representación 2_q como estados de la señal de salida A_{q1}, A_{q2}, A_{q3}, A_{q4}.

En el caso de que las señales de entrada E_{q1}, E_{q2}, E_{q3}, E_{q4} inicialmente formen un patrón de bits 0000, lo cual según la fila 1 de la tabla se representa en señales de salida 0100 y la señal de entrada Eq1 realice un cambio de estado, resulta como patrón de bits de salida según la segunda fila de la tabla anterior 1001. Es decir, que el cambio de estado de la señal de entrada Eq1 de 0 a 1 se “multiplica” con ayuda de la representación combinatoria K_q en las tres señales de salida A_{q1}, A_{q3} y A_{q4}, ya que la señal de salida Aq1 se modifica debido al cambio de estado de E_{q1} de 0 a 1, la señal de salida A_{q3} de 1 a 0 y la señal de salida A_{q4} de 0 a 1.

Un patrón de bits de entrada de 0010 da lugar un patrón de bits de salida 0011 (véase al respecto la tercera fila de la tabla). Partiendo de un patrón de bits 0000 y de un cambio de estado de la señal de entrada E_{q2} de 0 a 1, resultan por lo tanto igualmente cambios de estado en las tres señales de salida A_{q1}, A_{q2} y A_{q3}, aún cuando sólo se ha realizado un cambio de estado en el lado de entrada, en la señal de entrada E_{q2}.

Análogamente se detecta para patrones de bits de entrada 0100 y 1000, partiendo de 0000, que se modifican tres o los cuatro estados de salida. Investigaciones de la entidad solicitante relativas a todas las posibles variaciones de estado de señales de entrada individuales partiendo de todos los 16 patrones de bits de entrada, han dado como resultado que en la representación K_q que se ha representado, en promedio un cambio de estado o una variación de estado de una señal de entrada E_{qi} da lugar a 2,75 cambios de estado o variaciones de estado en señales de salida.

Por lo tanto en la transformación de las representaciones combinatorias como circuitos de conexión electrónicos, los flancos de señal que corresponden a los cambios de estado se someten a otros jitter y se "copian" en varias señales de salida, en el presente ejemplo en 2,75 señales de salida. En particular se transforma y se reproduce una señal de entrada afectada por jitter en varias señales de salida afectadas por jitter, completándose mediante la propia reproducción correspondiente jitter adicionales. El jitter, que se utiliza como fenómeno que aporta aleatoriedad, se distribuye así amplificado y en varios canales.

La representación combinatoria K_q reproducida como ejemplo en forma de tabla, puede representarse equivalentemente en forma de funciones booleanas.

Escrita como forma normal disyuntiva, la reproducción combinatoria Kq es:

$A_{q4}=$
$OR[AND(E_{q4},E_{q3},E_{q1}),$
$AND(E_{q4},NOT[E_{q3}],NOT[E_{q1}]),$
$AND(NOT[E_{q4}],E_{q3},NOT[E_{q1}]),$
$AND(NOT[E_{q4}],NOT[E_{q3}],E_{q1})],$

$A_{q3}=$
$OR[AND(E_{q4},NOT[E_{q3}],E_{q2}),$
$AND(E_{q4},NOT[E_{q2}],E_{q1}),$
$AND(NOT[E_{q4}],E_{q2},E_{q1}),$
$AND(NOT[E_{q4}],NOT[E_{q2}],NOT[E_{q1}])]$

$A_{q2}=$
$OR[AND(E_{q4},NOT[E_{q3}],NOT[E_{q2}]),$
$AND(NOT[E_{q4}],NOT[E_{q3}],E_{q2}),$
$AND(E_{q3},E_{q2},E_{q1}),$
$AND(E_{q3},NOT[E_{q2}],NOT[E_{q1}])]$

$A_{q1}=$
$OR[AND(E_{q4},NOT(E_{q3}),E_{q2},E_{q1}),$
$AND(E_{q4},NOT[E_{q3}],NOT[E_{q2}],NOT[E_{q1}]),$
$AND(NOT[E_{q4}],E_{q3},NOT[E_{q2}]),$
$AND(NOT[E_{q4}],E_{q3},E_{q1}),$
$AND(NOT[E_{q4}],NOT[E_{q3}],E_{q2},NOT[E_{q1}]),$
$AND(NOT[E_{q4}],NOT[E_{q2}],E_{q1}),$
$AND(E_{q3},NOT[E_{q2}],E_{q1})]$

Aquí OR es una combinación lógica „O“, AND es una combinación lógica ”Y“ y NOT es una combinación lógica “NO”. Para la implementación en cuanto a hardware, pueden realizarse las representaciones combinatorias, en vez de en base a una tabla look-up, también como combinación de puertas lógicas según la representación anterior. La representación de forma normal disyuntiva puede reescribirse también en una forma normal algebraica, que igualmente puede utilizarse para diseñar los correspondientes circuitos lógicos. Se puede escribir:

$A_{q4}=XOR[E_{q1},E_{q3},E_{q4}]$

$A_{q3}=NOT[XOR(E_{q1},E_{q2},E_{q4},AND[E_{q4},E_{q2},E_{q1}],AND[E_{q4},E_{q3},E_{q2}])]$

$A_{q2}=XOR[E_{q2},E_{q3},E_{q4},AND(E_{q3},E_{q1}),AND(E_{q4},E_{q3})]$

$A_{q1}=XOR[E_{q1},E_{q2},E_{q3},E_{q4},AND(E_{q3},E_{q1}),AND(E_{q3},E_{q2},E_{q1}),$
$AND(E_{q4},E_{q3},E_{q1}),AND(E_{q4},E_{q3},E_{q2})]$

Se observa en ambas representaciones que la señal de salida A_{q4} es independiente de un cambio de estado de la señal de entrada E_{q2}. Una estructura más optimizada aún de las representaciones combinatorias K_q prevé que una señal de salida correspondiente dependa de tantas señales de entrada como sea posible. Se preferiría especialmente que cada señal de salida de una representación combinatoria dependiese de todas las señales de entrada para la representación. Entonces se multiplicarían y amplificarían los jitter en las señales especialmente bien.

Las rutas de las señales o acoplamientos de las puertas combinatorias 2_1 a 2_{10} se indican simplemente de manera esquemática. Sólo entre las puertas 2_5 y 2_6 se representan explícitamente las cuatro líneas o uniones.

Ahora, una vez que el oscilador anular de cuatro pistas (n=4) oscila, por ejemplo la señal A_{51}, que se ha conducido como señal de entrada E_{61} a la puerta combinatoria 2_6, puede considerarse como señal que oscila aleatoriamente.

Un dispositivo de exploración 4 toma por ejemplo en la salida para la señal A_{51} el nivel que oscila y genera a partir del mismo un bit aleatorio ZB.

Investigaciones de la entidad solicitante han dado como resultado que aparecen curvas de señal aleatorias favorables también a igualdad de estados de entrada. Las figuras 3 a 6 muestran variantes de señales de bits aleatorias ZB, que se han generado con una implementación FPGA del circuito representado en la figura 2.

Sobre el eje y se representa el nivel de señal en voltios y sobre el eje x el tiempo en nanosegundos. Se utilizaron representaciones de bits biyectivas aleatorias n-en-n. Se observa que a igualdad de valores iniciales, ya después de un breve tiempo, por ejemplo después de 10 ns, resultan formas de señal completamente diferentes, que discurren aleatoriamente. Por lo tanto pueden utilizarse las formas de señal aleatorias como base para determinar valores de bits aleatorios.

La figura 7 muestra una representación esquemática de un tercer ejemplo de realización de un equipo para generar bits aleatorios. El equipo 100 implementa un cierto número de variantes opcionales de los equipos 1 y 10 descritos en relación con las figuras 1 y 2. El equipo 100 incluye cinco equipos de representación 2_1 - 2_5, que implementan en cada caso una representación combinatoria K_1 - K_5. Al respecto reproducen las representaciones K1 y K5 en cada caso cuatro señales de entrada en cuatro señales de salida. Así tienen los equipos de representación 2_1 y 2_5 entradas para cuatro señales de entrada E_{11} - E_{14} y E_{51} - E_{54} respectivamente y el mismo número de salidas para cuatro señales de salida de A_{11} - A_{14} y A_{51} - A_{54} respectivamente. Las representaciones K_2 y K_3 reproducen tres señales de entrada E_{21}, E_{22}, E_{23} y E_{31}, E_{32}, E_{33} respectivamente en cuatro señales de salida A_{21} - A_{24} y A_{31} - A_{34} respectivamente. La representación K_4 es una representación de cuatro en tres y genera a partir de cuatro señales de entrada E_{41} - E_{44} tres señales de salida A_{41}, A_{42}, A_{43}.

La señal de salida A_{23} se realimenta como señal de entrada E_{51} según se considere en alimentación y/o retroalimentación. Las señales de salida A_{13} y A_{14} se combinan lógicamente en Y con ayuda de una puerta Y 11 y se llevan como señal de entrada E_{23} al equipo de representación 22. Similarmente se combinan lógicamente en O las señales de salida A_{52} y A_{53} con ayuda de una puerta O11, se invierten con un inversor 8 y se llevan como señal de entrada E_{11} al equipo de representación 21. La señal de salida A_{31} se invierte con ayuda de un inversor 6 respecto a la señal de entrada E_{44}.

Resultan aquí varias realimentaciones tal que una variación de estado de al menos una señal de salida de un equipo de representación se lleva como una variación de estado de al menos una señal de entrada de otro equipo de representación. Además están realizadas las representaciones K_1 - K_5 tal que una variación de estado de una señal de entrada como promedio se reproduce en más de una señal de salida. Por ejemplo puede utilizarse para los equipos de representación K_1 y K_5 una representación biyectiva, tal como se ha descrito antes en relación con la tabla.

Un bucle de realimentación resulta por ejemplo a partir de las señales A_{14}, E_{23}, A_{23}, E_{51} y A_{51}, transmitiéndose en base a la configuración de las representaciones K_1, K_2 y K_5 flancos de señal también en otras rutas en el equipo 100 y provocando evoluciones de señal aleatorias.

Las señales A_{33} y A_{54} se toman en cada caso con ayuda de flip-flops toggle (de cambio de estado) 9. El correspondiente flip-flop T 9 sirve como contador, que computa los flancos de señal ascendentes como transiciones 0→1 módulo 2. En la salida de datos Q del flip-flop 9 puede tomarse entonces el correspondiente bit aleatorio.

El equipo propuesto y el procedimiento que sirve de base son especialmente adecuados para la implementación en ASICs. Las funciones lógicas de los equipos de representación tienen preferiblemente la misma profundidad lógica, para lograr el mismo tiempo de propagación de las representaciones combinatorias. A tablas lookup puede por lo tanto renunciarse también. La invención hace posible en consecuencia, entre otros, una rápida generación de bits aleatorios con un coste de hardware reducido.

Aún cuando la invención se ha ilustrado y descrito más en detalle mediante el ejemplo de ejecución preferente, la invención no queda limitada por los ejemplos dados a conocer y el especialista puede a partir de ello derivar otras variaciones sin abandonar el ámbito de protección de la invención.

REIVINDICACIONES

1. Equipo (1) para generar bits aleatorios (ZB) que incluye:
varios equipos de representación (2_1 - 2_m), estando preparado el equipo de representación (2_1 - 2_m) correspondiente para representar una cantidad n predeterminada de señales de entrada (E_{11} - E_{mn}), con ayuda de una representación combinatoria (K_1 – K_m), en una cantidad p predeterminada de señales de salida (A_{11} - A_{mp}),
en el que los equipos de representación (2_1 - 2_m) están encadenados entre sí y está configurado al menos un bucle de realimentación tal que una variación del estado de al menos una señal de entrada (Aij) de un equipo de representación (2i) se lleva como una variación del estado de al menos una señal de entrada (Ekl) a otro equipo de representación (2k),
caracterizado porque al menos una representación combinatoria (K_1 – K_m) está establecida tal que una variación de estado de una señal de entrada (E_{11} - E_{mn}) del correspondiente equipo de representación (2_1 - 2_m) en promedio se reproduce en más de una señal de salida (A_{m1} - A_{mp}) del correspondiente equipo de representación (2_1 - 2_m).

2. Equipo (1) de acuerdo con la reivindicación 1,
en el que al menos una representación combinatoria (K_1 – K_m) está establecida tal que las señales de entrada (E_{11} - E_{mn}) se reproducen, sometiéndolas a un jitter y a una función lógica, en las señales de salida (A_{11} - A_{mp}).

3. Equipo (1) de acuerdo con la reivindicación 1 ó 2,
en el que las representaciones combinatorias (K_1 – K_m) no implementan ninguna representación combinatoria que aporte una permutación de las señales de entrada (E_{11} - E_{mn}) en las señales de salida (A_{11} - A_{mp}).

4. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 3,
en el que los equipos de representación (2_1 - 2_m) están realizados tal que sus tiempos de propagación de la señal son iguales.

5. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 4,
en el que al menos un equipo de representación (2_1 - 2_m) incluye una tabla lookup (5_1 – 5_m) para implementar la representación combinatoria (K_1 – K_m).

6. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 5,
en el que al menos una representación combinatoria (K_q) corresponde a una biyección.

7. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 6,
en el que los equipos de representación (2_1 – 2_m) implementan en cada caso distintas representaciones combinatorias (K_1 – K_m).

8. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 7,
en el que los equipos de representación (2_1 - 2_m) encadenados entre sí constituyen un circuito de oscilador en anillo de varias pistas.

9. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 8
en el que el equipo incluye varios ramales de realimentación (3) de equipos de representación (2_1 - 2_m) encadenados.

10. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 9,
en el que el equipo (1) está realizado tal que cuando se realiza un acoplamiento de señales de entrada predeterminadas (E_{11} - E_{mn}), las señales de entrada predeterminadas (E_{11} - E_{mn}) son tales que el equipo (1) no se encuentra en un punto fijo.

11. Equipo (1) de acuerdo con una de las reivindicaciones 1 a 10,
que incluye además un dispositivo de exploración (4), para explorar una o varias señales de salida (A_{11} - A_{mp}) en salidas de uno o de distintos equipos de representación (2_1 - 2_m).

12. Equipo (1) de acuerdo con la reivindicación 11,
en el que el dispositivo de exploración (4) presenta un elemento de almacenamiento intermedio, en particular un T-flip-flop.

13. Equipo FPGA o equipo ASIC con un equipo de acuerdo con una de las reivindicaciones 1-12.

14. Procedimiento para generar bits aleatorios (ZB) en el que se realizan varias representaciones combinatorias (K_1 – K_m) encadenadas una tras otra, reproduciendo la correspondiente representación combinatoria (K_1 – K_m) una cantidad n predeterminada de señales de entrada (E_{11} - E_{mn}) en una cantidad p predeterminada de señales de salida (A_{11} - A_{mp}),

en el que al menos un bucle de realimentación está formado tal que una variación del estado de al menos una señal de entrada (A_{ij}) de una representación combinatoria (K_i) se lleva como una variación del estado de al menos una señal de entrada (E_{kl}) a otra representación combinatoria (K_k),
caracterizado porque al menos una representación combinatoria ($K_1 – K_m$) está elegida tal que una variación de estado de una señal de entrada ($E_{11} – E_{mn}$) se representa mediante la representación combinatoria ($K_1 – K_m$) en promedio en más de una señal de salida ($A_{11} – A_{mp}$).

15. Procedimiento de acuerdo con la reivindicación 14, en el que una señal de entrada ($E_{11} – E_{mn}$) correspondiente representa un valor de un bit.

FIG 1

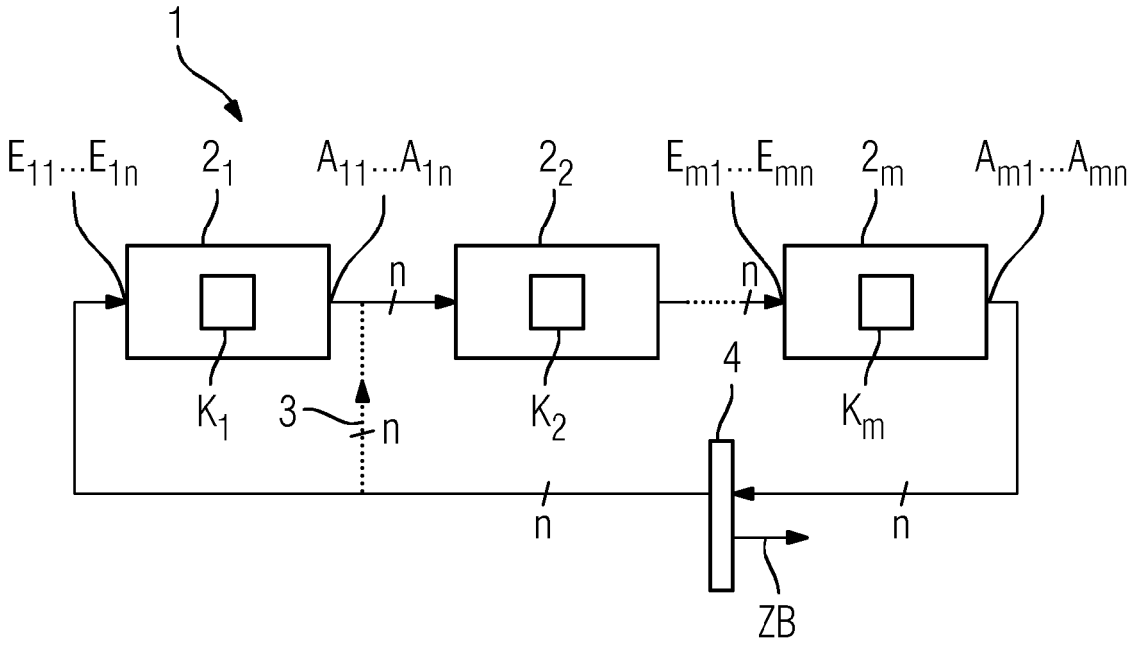

1
E11...E1n
21
A11...A1n
22
Em1...Emn
2m
Am1...Amn
n
n
K1
3
n
K2
Km
4
n
n
ZB

FIG 2

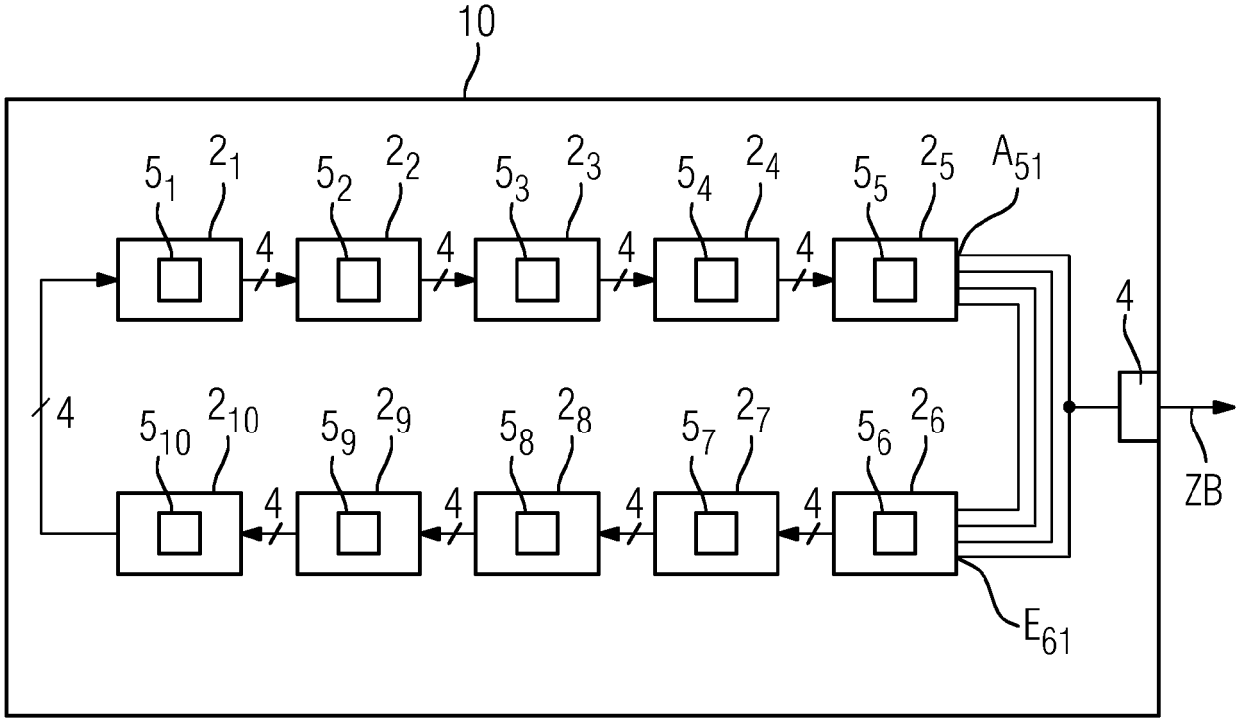

10
51
21
52
22
53
23
54
24
55
25
A51
4
4
4
4
4
4
510
210
59
29
58
28
57
27
56
26
4
4
4
4
4
ZB
E61

FIG 3

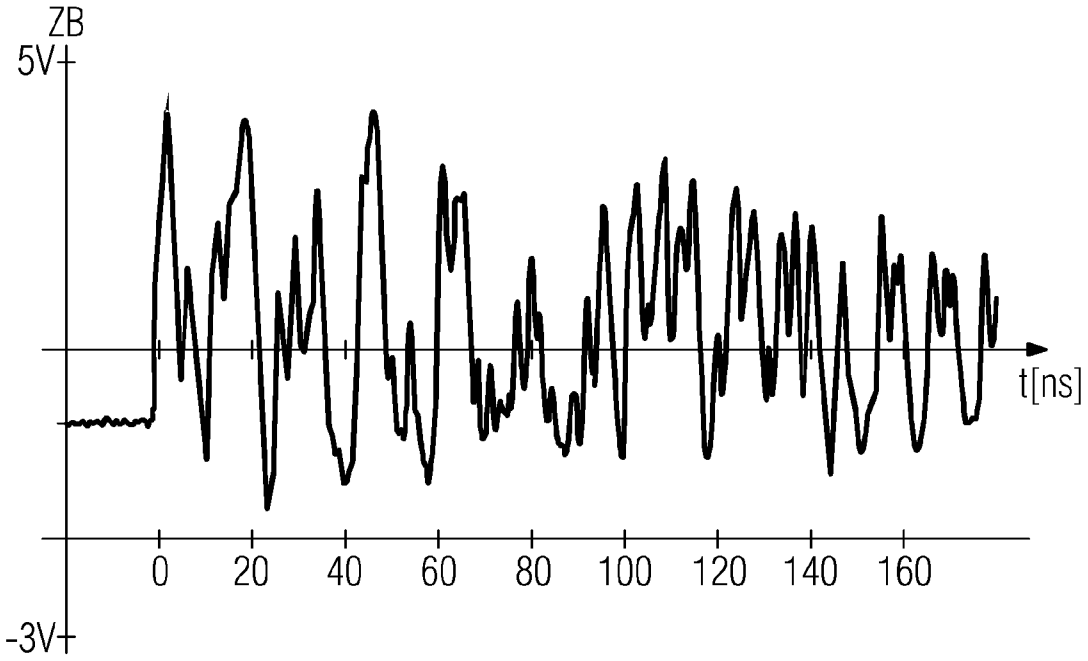

ZB
5V
-3V
t[ns]
0
20
40
60
80
100
120
140
160

FIG 4

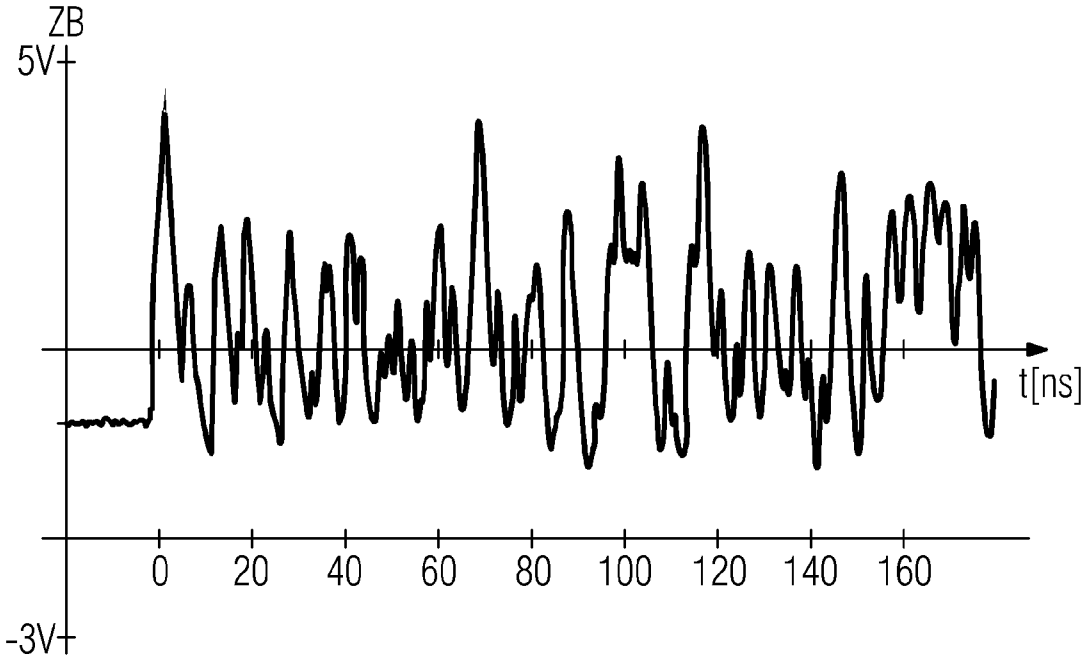

ZB
5V
-3V
t[ns]
0
20
40
60
80
100
120
140
160

FIG 5

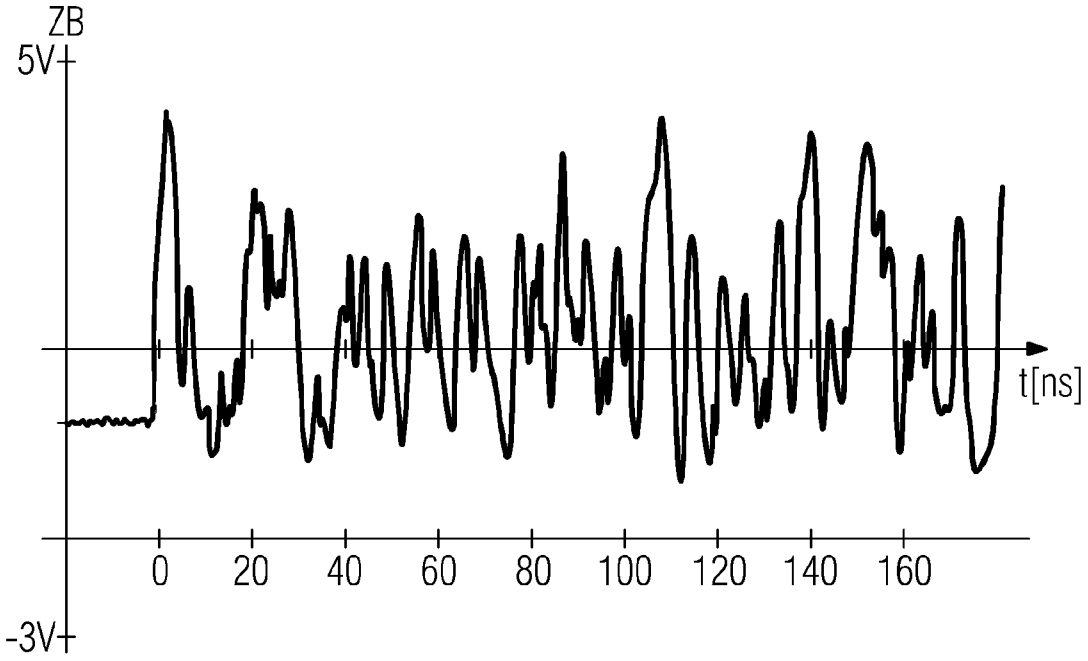

ZB
5V
-3V
t[ns]
0
20
40
60
80
100
120
140
160

FIG 6

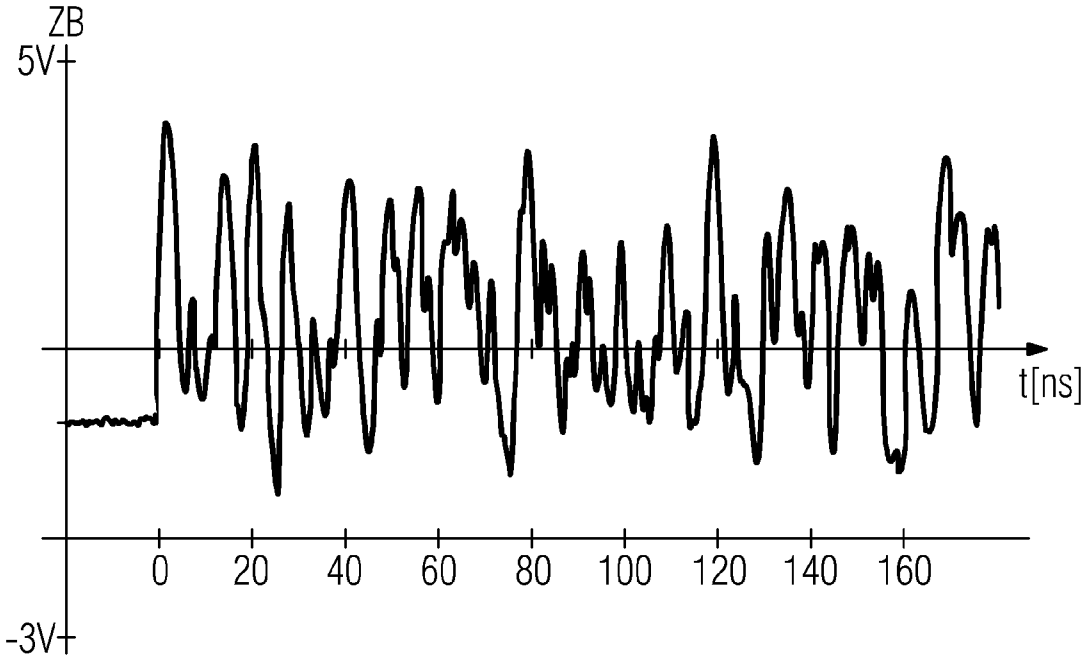
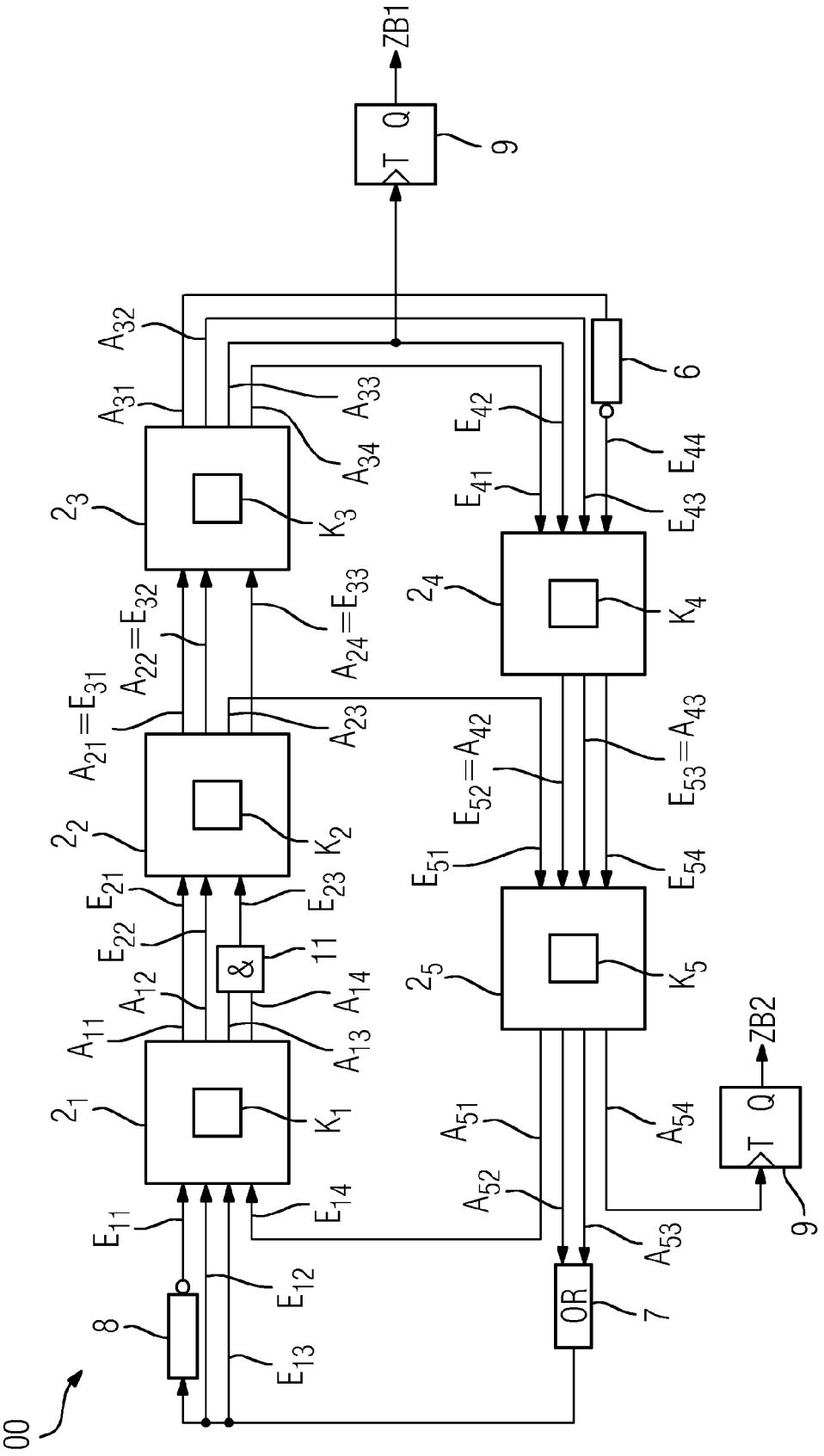

ZB
5V
-3V
t[ns]
0
20
40
60
80
100
120
140
160

FIG 7


100
8
OR
7
6
9
ZB1
ZB2
T Q
&
11
2_1
2_2
2_3
2_4
2_5
K_1
K_2
K_3
K_4
K_5
E_{11}
E_{12}
E_{13}
E_{14}
E_{21}
E_{22}
E_{23}
E_{41}
E_{42}
E_{43}
E_{44}
E_{51}
$E_{52}=A_{42}$
$E_{53}=A_{43}$
E_{54}
A_{11}
A_{12}
A_{13}
A_{14}
$A_{21}=E_{31}$
$A_{22}=E_{32}$
A_{23}
$A_{24}=E_{33}$
A_{31}
A_{32}
A_{33}
A_{34}
A_{51}
A_{52}
A_{53}
A_{54}