

REPUBLICA DE COLOMBIA



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-099010- -00000-0000

Fecha: 2014-05-08 16:13:56 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve. 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 7

PATENTE DE INVENCION

EXPEDIENTE No. _____

Contiene los documentos relativos a la solicitud de Patente de:

Título: MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN
DE NÚMEROS REALMENTE ALEATORIOS Y UN
SISTEMA DE JUEGO

Solicitante: NOVOMATIC AG

De GUMPOLDSKIRCHEN, AUSTRIA

Apoderado: MAURICIO JARAMILLO C.

Bogotá, D.C., Mayo de 2014

WF- 7329

 Industria y Comercio SUPERINTENDENCIA	SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO  No. 14-099010- -00000-0000 Fecha: 2014-05-08 16:13:56 Dep. 2020 DIR.NUEVASCR Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI Act. 411 PRESENTACION Folios: 7
---	--

DIRECCIÓN DE NUEVAS CREACIONES
SOLICITUD FASE NACIONAL -PCT

1	TIPO DE SOLICITUD	☒ Patente de invención ☒ Capítulo I	☐ Patente de Modelo de Utilidad ☐ Capítulo II
2	DATOS SOLICITUD INTERNACIONAL PCT (86)		
Solicitud Internacional No.		PCT/EP2012/072297	Fecha 09/11/2012
Publicación Internacional No.		WO2013068546	Fecha 16/05/2013
3	TÍTULO DE LA INVENCIÓN (200 caracteres o espacios máximos)		
MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN DE NÚMEROS REALMENTE ALEATORIOS Y UN SISTEMA DE JUEGO			
4	CLASIFICACIÓN INTERNACIONAL (CIP)		
G06F 7/58 (2006.01), H03K 3/84 (2006.01)			
5	SOLICITANTE (S) ☐ Esta persona también es inventor. Para datos adicionales utilizar hoja de información complementaria		
APELLIDOS O RAZÓN SOCIAL		NOMBRE	IDENTIFICACIÓN TIPO
1.	NOVOMATIC AG		
6	DATOS DEL SOLICITANTE		
DIRECCIÓN		Wiener Strasse 158, A-2352	No. TELÉFONO
CIUDAD		Gumpoldskirchen	CORREO ELECTRÓNICO
DEPARTAMENTO/ESTADO			NACIONALIDAD O LUGAR DE CONSTITUCIÓN
PAÍS DE RESIDENCIA		Austria	Austria
7	INVENTOR (ES) Para datos adicionales utilizar hoja de información complementaria		
APELLIDOS		NOMBRES	NACIONALIDAD
1.	HOMER	Alois	Austria
2.			
3.			
4.			
5.			
DIRECCIÓN DE CORREO ELECTRÓNICO:			
8	DATOS INVENTOR (ES)		
PAÍS RESIDENCIA		DEPARTAMENTO/ESTADO	CIUDAD DIRECCIÓN
1.	Austria		Gumpoldskirchen Wiener Strasse 158, A-2352
2.			
3.			
4.			
5.			
OTRO(S) SOLICITANTE(S) Y/O (OTRO(S)) INVENTOR(ES)			
☐ Los demás solicitantes y/o (demás) inventores se indican en una hoja a continuación.			
9	☐ REPRESENTANTE LEGAL ☒ APODERADO		
APELLIDOS		NOMBRES	IDENTIFICACIÓN
JARAMILLO CAMPUZANO		MAURICIO	C.C.80.421.942 T.P.74.555
DIRECCIÓN		Calle 67 NO. 7 – 35, oficina 1204	No. TELÉFONO 3192900
CIUDAD		Bogotá D.C.	CORREO ELECTRÓNICO jbenoit@gpzlegal.com
PAÍS		Colombia	No. RADICACIÓN DE PROTOCOLO DE PODER GENERAL

10	DECLARACIONES DE PRIORIDAD X SI ☐ NO			
(33) PAÍS DE ORIGEN 1.Unión Europea 2. 3.		CÓDIGO PAÍS EP	(31) NÚMERO 11008930.7	(32) FECHA (AAAA/MM/DD) 2011/11/09
11	DECLARACIÓN SOBRE USO DE RECURSOS GENÉTICOS O BIOLÓGICOS			
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de recursos genéticos o biológicos de los que cualquiera de los países miembros de la Comunidad Andina es país de origen.</i> ☐ SI X NO Nota: En caso afirmativo deberá anexar copia del contrato de acceso de recursos genéticos o productos derivados, o certificado o número de registro, expedido por la Autoridad competente.				
12	DECLARACIÓN SOBRE USO DE CONOCIMIENTOS TRADICIONALES			
<i>Declaro que el objeto de la presente solicitud de patente fue obtenido a partir de conocimientos tradicionales de comunidades indígenas, afroamericanas o locales de países miembros de la Comunidad Andina.</i> ☐ SI X NO Nota: En caso afirmativo deberá anexar la licencia o autorización de uso de conocimiento tradicional, o certificado, o número de registro expedido por la Autoridad competente.				
13	REDUCCIÓN DE TASAS			
<i>Declaro que carezco de medios económicos para presentar la solicitud de patente.</i> ☐ SI X NO Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.				
Micro, pequeñas y medianas empresas ☐				
Universidades públicas o privadas ☐				
Entidades sin ánimo de lucro ☐				
Debe aportar los documentos que se indican en el numeral 17 de anexos				
14	AUTORIZACIÓN DE NOTIFICACIÓN EN LÍNEA ☐ SI X NO			
Manifiesto que he leído y entendido perfectamente los términos y condiciones de uso de medios electrónicos para las notificaciones en línea a través de Internet de los actos administrativos proferidos por la Superintendencia de Industria y Comercio que deben ser notificados personalmente y, en consecuencia, autorizo el servicio de notificación a través de internet.				
15	COMPROBANTE DE PAGO O PAGO ELECTRÓNICO	N°	Fecha	
16	FIRMA DEL SOLICITANTE, DEL APODERADO O DEL REPRESENTANTE LEGAL <i>Junto a cada firma, indicar el nombre del firmante y su calidad (si tal calidad no es obvia al leer el petitorio)</i>			
17	ANEXOS			
Documentación Técnica Solicitud Internacional en castellano		Documentación Jurídica		
1. X Descripción N° de folios: 43		9. X Poderes, si fuera el caso. Exp. No. 12-93139		
2. X Reivindicaciones N° Reivindicaciones: 15		10. ☐ Documento que legalmente pruebe la cesión del inventor al solicitante o a su causante.		
3. X Dibujos y/o figuras N° folios: 5		11. ☐ Copia del contrato de acceso de recursos genéticos o productos derivados, certificado o número de registro, si fuera el caso.		
4. X Resumen.		12. ☐ Copia de la licencia o autorización de Conocimientos Tradicionales, certificado o número de registro, si fuera el caso.		
5. ☐ Certificado de depósito de material biológico si fuera el caso.		13. Reducción de tasas		
6. ☐ Listado de secuencias de nucleótidos y/o aminoácidos en forma digital si fuera el caso.		Micro, pequeñas o medianas empresas		
7. ☐ Arte final 12 x 12.		☐ Copia simple de la declaración de renta del año inmediatamente anterior, o en su defecto prueba documental idónea.		
8. ☐ Anexo formato digital.		☐ Documento de constancia de cumplimiento con lo establecido en la ley 905 de 2004.		
		Universidades públicas o privadas		
		☐ Copia acto de reconocimiento institucional emitido por el Ministerio de Educación		
		Entidades sin ánimo de lucro		
		☐ Copia de registro vigente en Cámara de comercio.		
		☐ Hoja de información complementaria.		
		☐ Otros, especificar		
		14. X Comprobante de pago de la tasa de presentación de la solicitud.		
		15. ☐ Comprobante de pago por reivindicación de prioridad.		
		16. ☐ Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación.		
		17. X Comprobante de pago por reivindicación adicional a 10.		

	EXTRACTO PARA PUBLICACIÓN ☐ Patente de Invención ☐ Patente modelo de utilidad ☒ PCT
---	---

(21) No. de solicitud:	(51) int. Cl: G06F 7/58 (2006.01), H03K 3/84 (2006.01)
(22) Fecha de solicitud:	(71) Solicitante(s): NOVOMATIC AG
(30) Prioridad:	(72) Inventor(es): Alois HOMER
(31) No. Prioridad: 11008930.7	
(32) Fecha: 09/11/2011	
(33) País: Unión Europea	(74) Apoderado(s): MAURICIO JARAMILLO CAMPUZANO
(54) Título: MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN DE NÚMEROS REALMENTE ALEATORIOS Y UN SISTEMA DE JUEGO	
Las casillas identificadas con 85, 86 y 87 sólo aplican para PCT	
(85) Fecha límite inicio Fase Nacional: 09/06/2014	
(86) Datos relativos a la presentación de la solicitud PCT	(87) Publicación internacional
Fecha: 09/11/2012	Fecha: 16/05/2013
No. de solicitud PCT: PCT/EP2012/072297	No. Publicación: WO2013068546

Resumen reivindicación (es):

Un dispositivo para generar números realmente aleatorios mediante un proceso de óptica cuántica, comprendiendo el dispositivo: una fuente de luz para generar al menos un fotón único dentro de un haz de luz; y al menos dos detectores para detectar cada uno de ellos fotones únicos dentro del haz proporcionando de este modo señales del detector; y medios de control; en donde cada uno de los detectores para detectar fotones únicos comprende al menos un punto cuántico; y en donde los detectores se sitúan en una posición espacial sustancialmente equivalente de probabilidad de detección de los fotones únicos en el haz; y en donde los medios de control se proporcionan y adaptan para controlar la generación de una serie de fotones únicos y para registrar las señales del detector para generar valores de números realmente aleatorios.

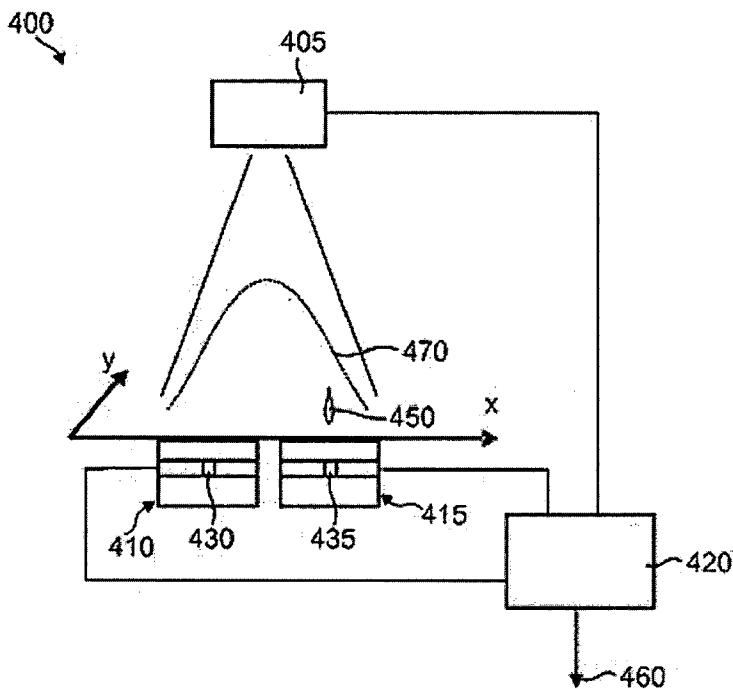


FIG. 4

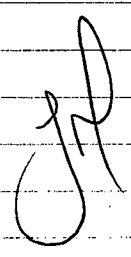
4

 Industria y Comercio SUPERINTENDENCIA		PLANILLA DE RADICACIÓN - DIGITALIZACIÓN DIARIA RELACIÓN DE ANEXOS	
Dependencia: 2020		Fecha: <u>2014</u> / <u>05</u> / <u>08</u> AAAA MM DD	
		Recorrido: 4	
Tipo de Radicación: Entrada: ☒ Salida: ☐ Traslado: ☐ Convenio: ☐			
Radicador:		Planilla:	

ID	No. Radicación	Consecutivo	Item
1	14-99010	0	7
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Item	Unidad de Conservación
1	Bolsa
2	Caja
3	Libro
4	Sobre
5	Tomo
6	Otro
Item	Soporte Documental
☒	CD
8	Disquete
9	DVD
10	Folleto
11	Foto
12	Periódico
13	Plano
14	Publicación Periódica
15	USB
16	Otro

Observaciones: EL CD ANEXO CONTIENE UN TOTAL DE 1 ARCHIVO: 1 EN FORMATO PDF, EL CUAL FUE PROCESADO EL CD SE ENCUENTRA EN EL FOLIO 4
--



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

-/-

2329

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0042792

Bogotá D.C., Abril 23 de 2014 - 15:00:05

RECIBIDO DE : GOMEZ PINZON ASEMARCAS S.A.

NI 830.121.797

RE

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	598477412	22/04/2014	16.891.000.00
CONSIGNACION	BANCO DE BOGOTA	062754387	610930865	23/04/2013	21.000.00

*** Conceptos Pagados ***

CANT. RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
1 50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	515.000.00	515.000.00
			\$515.000.00

SON: **QUINIENTOSQUINCE MIL PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-099010- -00000-0000

Fecha: 2014-05-08 16:13:56 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 17

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C. - Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

, Abril 23 de 2014 - 15:00:10

5
A

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

-/-

7329

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0042793

Bogotá D.C., Abril 23 de 2014 - 15:00:05

RECIBIDO DE : GOMEZ PINZON ASEMARCA S.A.

NI 830.121.797

RE

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	598477412	22/04/2014	16.891.000.00
CONSIGNACION	BANCO DE BOGOTA	062754387	610930865	23/04/2013	21.000.00

*** Conceptos Pagados ***

CANT. RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
5 50005-01-01 SOLICITUDES	1607 REIVINDICACION PATENTE UNITARIA ADICIONAL A LAS 10 INIC	31.000.00	155.000.00
			\$155.000.00

SON: **CIENTO CINCUENTA Y CINCO MIL PESOS MONEDA CORRIENTE***

Responsable:

-*****-

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 14-099010- -00000-0000

Fecha: 2014-05-08 16:13:56 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 6

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.slc.gov.co e-mail: info@slc.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

, Abril 23 de 2014 - 15:00:10

6

5



No. 14-099010- -00000-0000

Fecha: 2014-05-08 16:13:56 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 411 PRESENTACION Folios: 7

PATENTE DE INVENCION ☐

MODELO

☐	Indicación que se solicita una patente.
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Descripción de la invención
☐	Dibujos de ser estos pertinentes
☐	Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)
Completa ☐	Incompleta ☐

PATENTE DE INVENCION PCT ☒ MODELO DE UTILIDAD PCT ☐ Art.33 Decisión 486/00, Circular Única

☒	Indicación que se solicita una PCT
☒	Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)
☐	Dibujos de ser estos pertinentes
☒	Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)
Completa ☒	Incompleta ☐

DISEÑO INDUSTRIAL ☐

(Art. 119 Decisión 486/00)

☐	Indicación que se solicita Diseño industrial
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica y fotográfica del Diseño industrial o muestra del material que incorpora el diseño
☐	Comprobante de pago de las tasas establecidas
Completa ☐	Incompleta ☐

ESQUEMA DE TRAZADO ☐

(Art. 92 Decisión 486/00)

☐	Indicación que se solicita un esquema de trazado
☐	Datos de identificación del solicitante o de la persona que presenta la solicitud
☐	Representación gráfica de un esquema de trazado
☐	Comprobante de pago de las tasas establecidas
Completa ☐	Incompleta ☐

MÉTODO Y DISPOSITIVO PARA LA GENERACIÓN DE NÚMEROS
REALMENTE ALEATORIOS Y UN SISTEMA DE JUEGO

CAMPO DE LA INVENCION

Esta invención está relacionada en general con el campo
5 de la generación de números aleatorios y, más en particular,
con un método y un dispositivo para generar números realmente
aleatorios basado en un proceso de óptica cuántica. Aún más
en particular, la presente invención está relacionada con la
generación de números realmente aleatorios mediante la
10 mecánica cuántica para sistemas de juego.

ANTECEDENTES DE LA INVENCION

Los números aleatorios son de una enorme importancia en
muchas aplicaciones. En criptografía, por ejemplo, es
necesario utilizarlos, respectivamente, para la generación de
15 claves criptográficas o la inicialización de ciertas
variables en los protocolos criptográficos. También se pueden
encontrar aplicaciones en diversos otros campos como, por
ejemplo, simulaciones numéricas y estadísticas.

En la industria del juego, las máquinas de juego
20 actuales utilizan generadores de números pseudo aleatorios
para determinar apuestas y premios. El generador de números
pseudo aleatorios utiliza un algoritmo matemático
determinista que genera una secuencia de números
"aparentemente" aleatorios. Sin embargo, tal y como implica
25 el término "pseudo", la secuencia de números generada por el
generador de números pseudo aleatorios no es realmente
aleatoria. Los números pseudo aleatorios se generan
utilizando un algoritmo aritmético que produce como resultado
números que pueden pasar la mayor parte de test estadísticos
30 de aleatoriedad. Estos algoritmos toman como entrada un
parámetro de inicialización conocido como semilla y generan

números de forma iterativa. Sin embargo, es completamente determinista y eventualmente se repite. Dada la variable que determina la secuencia, los números son predecibles (con mayor o menor esfuerzo) lo cual provoca que también se puedan
5 predecir los resultados de las apuestas de un juego basado en apuestas, lo cual también puede provocar que el sistema sea vulnerable a ataques ilegales.

Las regulaciones de la industria de la lotería y el juego requieren que los números aleatorios que se utilizan
10 para jugar a los juegos de azar pasen ciertos test mínimos de aleatoriedad estadística para asegurar la imparcialidad y evitar la alteración no autorizada de los números aleatorios. Las regulaciones también requieren que se auditen los números aleatorios utilizados; un casino debe ser capaz de verificar
15 que la secuencia de números aleatorios, la cual provoca un premio gordo enorme, se ha originado a partir de un generador de números aleatorio autorizado perteneciente al casino o al operador de lotería.

Los generadores de números realmente aleatorios son
20 dispositivos que utilizan un proceso físico para producir números realmente aleatorios. Para la generación de números realmente aleatorios se pueden utilizar numerosos procesos físicos como fuente de aleatoriedad.

La aleatoriedad se encuentra implícita en un nivel
25 fundamental de la física cuántica. En consecuencia, tiene sentido utilizar un proceso descrito por la física cuántica como fuente de aleatoriedad para la generación de números realmente aleatorios.

La patente de los EE.UU. número 6,249,009 divulga un
30 generador de números realmente aleatorios que utiliza mecánica cuántica con un láser, un filtro de densidad neutra,

y un único tubo fotomultiplicador que detecta fotones. Otros modos de realización de un generador de números realmente aleatorios pueden tener un láser, un filtro de densidad neutra, un divisor de haz, y dos tubos fotomultiplicadores
5 cada uno de los cuales detecta un solo fotón del divisor de haz.

Lo que se necesita es utilizar un proceso de óptica cuántica mejorado como base para la generación de números realmente aleatorios. Además, se necesita un generador de
10 números realmente aleatorios simple y práctico basado en un proceso de óptica cuántica.

OBJETO Y RESUMEN DE LA INVENCION

Uno de los objetos de la invención es proporcionar un dispositivo y un método del tipo mencionado en el primer
15 párrafo, el cual evite los inconvenientes descritos más arriba.

Para conseguir el objeto descrito más arriba, se proporcionan las características diferenciales de acuerdo con la invención utilizando un dispositivo de acuerdo con la
20 invención de modo que un dispositivo de acuerdo con la invención se pueda describir del siguiente modo:

Un dispositivo para generar números realmente aleatorios mediante un proceso de óptica cuántica, comprendiendo el dispositivo: una fuente de luz para generar al menos un fotón
25 único dentro de un haz de luz; y al menos dos detectores para detectar cada uno fotones únicos dentro del haz proporcionando por lo tanto señales de detección; y medios de control; en donde los detectores para detectar los fotones únicos comprenden cada uno al menos un punto cuántico; y en
30 donde los detectores se sitúan en una posición espacial sustancialmente equivalente de probabilidad de detección de

fotones únicos en el haz; y en donde los medios de control se proporcionan y adaptan para controlar la generación de una serie de fotones únicos y para registrar las señales de detección con el fin de generar los números realmente
5 aleatorios.

La provisión de las características diferenciales de acuerdo con la invención proporciona ventajas de que en particular, evitando el proceso de avalancha y sus problemas asociados, la generación de números aleatorios es menos
10 propensa al ruido de cuenta de oscuridad, en particular cuando se opera en altas frecuencias. Además, como el detector está basado en un transistor, el elemento principal del circuito electrónico de alta velocidad puede tener una respuesta rápida en el tiempo. Otra ventaja es que el
15 detector del punto cuántico es capaz de funcionar en tensiones bajas de funcionamiento (por ejemplo menos de 5 Voltios) y es más robusto. También es apto para la fabricación en una disposición de detectores multicanal.

A diferencia de los generadores de números aleatorios
20 basados en detectores de un fotón único de estado sólido orientados a fotodetectores de avalancha en modo Geiger, el sistema de acuerdo con la presente invención evita las desventajas inherentes al proceso de avalancha que impiden la realización de generadores cuánticos de números aleatorios
25 fiables y rápidos. Algunas de estas limitaciones físicas implícitas son: Limitaciones del Material: casi todos los semiconductores mixtos que pueden proporcionar detectores de longitud de onda mayores tienen una baja tasa de ionización y, por lo tanto, un bajo rendimiento. Altas Tasas de Tunelado
30 y de Generación: los campos eléctricos elevados provocan una alta tasa de tunelado, incluso en el material de espacio de

banda ancha, y la corriente de tunelado se convierte en la fuente principal de la cuenta de oscuridad en los detectores de fotones de avalancha modernos. Además, la región de avalancha consumida completamente produce el máximo ruido de
5 generación Shockley-Read-Hall. Uniformidad Baja: una parte de la variación porcentual del dopaje o del espesor de la capa puede dar como resultado cambios apreciables en la ganancia, al corriente de oscuridad, la tensión de ruptura y la respuesta en frecuencia. Las variaciones de temperatura y
10 polarización evitarían la materialización de una matriz de 2D grande. Alta Emisión de Fotones: las portadoras de energía (calientes) que son necesarias para el proceso de avalancha también producen fotones. De hecho, los detectores basados en avalancha también se conoce que producen "destellos de
15 fotones" que son tres o cuatro órdenes de magnitud más brillantes que el haz de entrada. Los fotones producidos pueden interferir gravemente con el resto de componentes del sistema en un detector de fotón único de un único elemento, y producir una interferencia significativa en una disposición
20 de detectores de fotones de fotón único.

Para conseguir el objeto definido más arriba, las características diferenciales de acuerdo con la invención se proporcionan con un método de acuerdo con la invención, de modo que un método de acuerdo con la invención se puede
25 caracterizar del siguiente modo:

Un método para generar un número aleatorio, comprendiendo los pasos del método, proporcionar una disposición de al menos dos detectores e iluminarlo mediante un haz de luz que comprende un fotón único; y detectar el
30 fotón único utilizando al menos dos detectores de la disposición teniendo cada detector un punto cuántico y

estando asociado con valores; y generar el número aleatorio en función de los valores asociados con la detección del detector del fotón único.

Estos y otros aspectos de la invención son evidentes a partir de los modos de realización descritos a continuación y se aclararán haciendo referencia a ellos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describirá con más detalle la invención, mediante un ejemplo no limitante, haciendo referencia a los modos de realización que se muestran en los dibujos.

La Fig. 1 muestra una máquina de juego.

La Fig. 2 muestra un diagrama de bloques de los componentes en un dispositivo generador de números realmente aleatorios para su utilización en un dispositivo de máquina de juego de acuerdo con otro ejemplo de modo de realización de la invención.

La Fig. 3 es un diagrama de bloques del circuito de un dispositivo de acuerdo con todavía otro ejemplo de modo de realización de la invención.

La Fig. 4 muestra un dispositivo para generar números realmente aleatorios mediante un proceso de óptica cuántica de acuerdo con un ejemplo de modo de realización de la invención.

La Fig. 5 muestra una estructura de las capas de un detector de fotones únicos de acuerdo con la presente invención.

DESCRIPCIÓN DE LOS MODOS DE REALIZACIÓN

La FIG. 1 muestra una máquina 50 de juego que tiene una ventana terminal 10 para mostrar una pantalla 14a de un juego de rodillos. La máquina 50 de juego dispone varios modos de

funcionamiento del juego. Inicialmente la máquina 50 de juego opera en un modo de funcionamiento estándar del juego hasta que sucede un evento aleatorio y, a continuación la máquina 50 de juego puede operar en un modo de funcionamiento 5 característico del juego. En el modo de funcionamiento estándar del juego se muestra una matriz de símbolos en un formato que incluye cinco rodillos orientados en columnas y tres filas horizontales. En un modo de realización los rodillos son rodillos físicos que giran, y en otro modo de 10 realización los rodillos son imágenes de rodillos físicos.

La pantalla 14a está configurada para mostrar una matriz 26 de símbolos que imitan los rodillos mecánicos de máquinas tragaperras en el modo de funcionamiento estándar del juego de acuerdo con un aspecto de la invención. En consecuencia, 15 cada columna de la matriz de símbolos imita un único rodillo mecánico de una máquina tragaperras. La ventana terminal 10 está inclinada con respecto al suelo para quedar frente a un usuario.

En otro modo de realización de la invención, la pantalla 20 14a incluye rodillos mecánicos de máquina tragaperras. Se puede apreciar que en la presente solicitud se contemplan configuraciones híbridas que tienen tanto componentes mecánicos como digitales. La pantalla 14b es informativa para facilitar que se pueda resaltar cualquiera de los distintos 25 símbolos, y las líneas ganadoras para facilitar la ejecución del juego.

La matriz 26 de símbolos dispone de tres filas y cinco columnas. Sin embargo, la matriz 26 de símbolos puede incluir cualquier número de filas y columnas en función de varios 30 formatos de juegos. Tal como se muestra, la matriz 26 de

símbolos incluye una pluralidad de símbolos 24a, 24b, 24c y 24d, y tres símbolos multiplicadores 24e, 24f y 24g.

La máquina 50 de juego incluye el hardware y los dispositivos periféricos necesarios para el funcionamiento de la máquina de juego. Los dispositivos periféricos en el presente modo de realización comprenden: una impresora 51, un monedero 52, un billeteero 53, una caja 54 de seguridad, un dispositivo 62 lector de tarjetas, y altavoces 60.

La máquina 50 de juego incluye una placa base 55 que comprende un procesador central 56, una memoria electrónica 57 para almacenar instrucciones del procesador y una unidad 58 de disco duro para almacenar software. La memoria 57 y la unidad lectora de disco duro están adaptadas para comunicarse con el procesador central 56.

El billeteero 53 está adaptado para recibir dinero y para enviar el dinero a la caja 54 de seguridad. El lector 62 de tarjetas lee tarjetas de pago incluyendo tarjetas inteligentes, tarjetas de crédito, tarjetas de débito y similares. El lector 62 de tarjetas y el billeteero comunican las transacciones económicas al procesador 56. Tanto la ventana 10 del terminal como los altavoces 60 comunican instrucciones y resultados al jugador (usuario).

El lector 62 de tarjetas está colocado cerca de la ventana 10 del terminal para facilitar el uso con el fin de permitir que un usuario pueda utilizar el lector 62 de tarjetas cuando se encuentra sentado o de pie.

La ventana 10 del terminal preferiblemente es un monitor con pantalla táctil que dispone de cuatro componentes básicos, los cuales incluyen un sensor táctil, un monitor (pantalla), un controlador y un controlador de software. El sensor táctil está, por ejemplo, basado en tecnología

Capacitiva, Resistiva, Onda Acústica de Superficie (SAW)/Onda Acústica Rasante (GAW) u otras similares. El monitor, por ejemplo, está basado en tecnología de Tubo de Rayos Catódicos (CRT), Pantalla de Cristal Líquido (LCD), plasma u otras
5 tecnologías similares que dispongan de una pantalla de visualización en la que se pueda instalar el sensor. El controlador recibe entradas desde el sensor táctil y lleva a cabo operaciones como respuesta al procesador central 56. El controlador software permite al controlador y al procesador
10 central 56 que se comuniquen y permite al controlador reconocer la entrada detectada por el sensor táctil.

El procesador central 56 y la placa base 55 forman parte, preferiblemente, de un ordenador de propósito general que dispone de una unidad de monitor de vídeo con
15 Entradas/Salidas (E/S) de vídeo a la interfaz de vídeo del monitor de la pantalla táctil, al menos una salida de audio con E/S de audio a un altavoz 60a de sonido, un sistema operativo de ordenador, por ejemplo, Windows™, Linux™, Unix™ o similares, controladores software para todos los
20 periféricos de E/S, y puertos serie/paralelo y/o USB para la conexión a periféricos tales como, por ejemplo, una impresora, un dispositivo lector de tarjetas inteligentes e interfaces de Datos de E/S y conversores/divisores de Datos de E/S, donde sea necesario.

25 En la unidad 58 de disco duro, u otra unidad de memoria de almacenamiento equivalente, se almacena un programa software de ordenador. El programa puede organizar la visualización de todos los componentes del juego en una Interfaz Gráfica de Usuario (GUI) sobre el monitor de la
30 pantalla táctil. El programa puede filtrar los datos relevantes para actuar, interpretar el significado de los

datos (después de una conversión de datos si es necesario) teniendo en cuenta algunas veces un evento anterior, el estado actual o un evento previsto, y actuar en función de la interpretación. Los datos pueden provenir de las interfaces de E/S de todos los dispositivos/el equipo conectados al programa. Se toma el ejemplo de determinar la posición del contacto de un usuario sobre un punto en el espacio de un componente gráfico sobre un monitor de pantalla táctil. El controlador de la pantalla táctil puede convertir una coordenada correspondiente a cada uno de los puntos táctiles en una cadena de datos binarios. A continuación, los datos se pueden transferir a través de conexiones en serie desde el controlador al procesador central. El procesador central puede extraer los datos, leer las coordenadas y llevar a cabo la acción asociada con el lugar tocado.

La FIG. 2 es un diagrama de bloques de los componentes de una máquina de juego y un dispositivo generador de números realmente aleatorios utilizado en la misma de acuerdo con un modo de realización de la presente invención. El conjunto 202 de circuitos principal puede controlar las comunicaciones entre los componentes del dispositivo. El conjunto 202 de circuitos principal puede tener un concentrador de controlador de memoria (MCH) o puente norte 204 y un concentrador de controlador de entradas/salidas (E/S) (ICH) o puente sur (206). El conjunto 202 de circuitos principal puede combinar todas las características del ICH con un puerto gráfico de aceleración (AGP) y conectarse directamente al procesador. Las funciones de un conjunto 202 de circuitos principal y de los puentes norte 204 y sur 206 son conocidas en la técnica y no se describirán en detalle en la presente solicitud. Aunque las figuras ilustran componentes

específicos acoplados al conjunto 202 de circuitos principal, son ejemplos de componentes para un modo de realización de la invención y no pretenden ser una limitación ya que se pueden utilizar otros componentes.

5 Un generador 400 de números realmente aleatorios de acuerdo con la presente invención que se muestra en la Fig. 4 con más detalle está acoplado al procesador 210 a través del conjunto 202 de circuitos principal en el puente sur 206. El generador 400 de números realmente aleatorios puede generar,
10 por ejemplo, 600 kilobits de números realmente aleatorios por segundo. Una memoria de acceso aleatorio (RAM) 212 se puede acoplar al procesador 210 a través del conjunto 202 de circuitos principal en el puente norte 204 para almacenar y procesar los números realmente aleatorios generados por el
15 generador 400 de números realmente aleatorios. Los números realmente aleatorios se pueden almacenar en la RAM 212 y ser procesados por el procesador 210. El procesamiento de los números realmente aleatorios puede implicar la verificación de la integridad hardware del generador 400 de números
20 realmente aleatorios, eliminar sesgos, comprobar la aleatoriedad, aprobar, firmar digitalmente, verificar digitalmente, cifrar, descifrar, y/o auditar los números aleatorios, tal como se describirá en detalle más abajo. Después del procesamiento, los números aleatorios se pueden
25 almacenar en la RAM 212.

 El dispositivo 200 también puede incorporar un dispositivo 214 de almacenamiento de números aleatorios acoplado al procesador 210 a través del conjunto 202 de circuitos principal en el puente sur 206. Para el
30 almacenamiento de los números realmente aleatorios se puede utilizar el dispositivo 214 de almacenamiento de números

aleatorios en lugar de la RAM 212. El dispositivo 214 de almacenamiento de números aleatorios puede ser un dispositivo de almacenamiento masivo, como por ejemplo una unidad de disco duro o una unidad flash, utilizado en un ordenador de propósito general que típicamente permite que se pueda leer código y datos desde y escribirlos en el dispositivo de almacenamiento masivo. Sin embargo, en un entorno de máquina de juego, la modificación del código del juego almacenado en un dispositivo de almacenamiento masivo está estrictamente controlada y únicamente se permitiría bajo eventos específicos de tipo mantenimiento siendo necesarios habilitadores electrónicos y físicos. Aunque este nivel de seguridad se podría proporcionar mediante software, los ordenadores de juego que incluyen dispositivos de almacenamiento masivo incluyen preferiblemente un circuito de protección de datos a nivel de hardware del almacenamiento masivo que funciona a nivel de circuito para controlar los intentos de modificación de datos en el dispositivo de almacenamiento masivo y generar avisos de error tanto software como hardware si se intentara una modificación de datos sin encontrarse presentes los habilitadores electrónicos y físicos apropiados.

Un controlador de vídeo o un adaptador de pantalla 216, como por ejemplo una tarjeta gráfica o de vídeo, a una pantalla 220 y al procesador 210 se les puede acoplar a través del conjunto 202 de circuitos principal en el puente norte 204. El adaptador de pantalla 216 puede permitir que los mensajes del procesador 210 sean mostrados en la pantalla 220. En un modo de realización, el adaptador de pantalla 216 se puede integrar dentro del puente norte 204. La pantalla 220 puede ser cualquier tipo de pantalla, por ejemplo, una

pantalla de cristal líquido (LCD), una pantalla fluorescente, una pantalla de tubo de rayos catódicos (CRT), y similares. Esto permite que el dispositivo pueda mostrar errores internos o aciertos originados en el propio hardware y/o software del dispositivo. Por ejemplo, si falla el generador 5 400 de números realmente aleatorios, se mostrará un mensaje de error informando al usuario sobre el fallo. Adicionalmente, si una acción tiene éxito, como por ejemplo la validación de una secuencia de números aleatorios frente a un premio gordo exigido, se puede mostrar un mensaje de 10 "validación satisfactoria" en la pantalla 220. También se puede mostrar otra información como, por ejemplo, la fecha y hora en la que se generaron y/o transmitieron los números aleatorios, la identificación única del dispositivo de juego remoto al que se transmitieron los números aleatorios y 15 cualquier otra información.

Ahora bien, es conocido que el dispositivo 200 no necesita disponer de una pantalla 220 y/o un adaptador de pantalla 216. En su lugar, en otro modo de realización, el 20 dispositivo 200 puede mostrar mensajes en un servidor de juego remoto como, por ejemplo, la pantalla del servidor de juego remoto. Los mensajes se pueden transmitir a través de la interfaz 222 de E/S. Una aplicación de consola en el servidor de juego remoto se puede comunicar con el procesador 25 210 a través de la interfaz 222 de E/S y los mensajes de monitorización enviados al servidor de juego remoto desde el procesador 210.

Tal como se ha descrito más arriba, se puede utilizar una interfaz 222 de E/S para comunicarse con el servidor de 30 juego remoto. La interfaz 222 de E/S también se puede acoplar al procesador 210 a través del conjunto 202 de circuitos

principal en el puente sur 206 para recibir peticiones y transmitir datos a un dispositivo de juego remoto. La interfaz 222 de E/S puede ser cualquier tipo de interfaz como, por ejemplo, un transceptor inalámbrico, un bus serie universal (USB), una interconexión de componentes periféricos (PCI), una tarjeta de red, un bus de datos, o cualquier otro tipo de interfaz que permita que el dispositivo 200 de generación de números realmente aleatorios se comuniquen con el servidor de juego remoto. El servidor de juego remoto puede ser, pero no se limita a, un ordenador personal, una máquina tragaperras, un dispositivo de juego remoto, un dispositivo de juego portátil como, por ejemplo, pero no limitado a, un teléfono móvil, un asistente digital personal y una consola de juego inalámbrica, o cualquier otra máquina de juego. La interfaz 222 de E/S también se puede conectar a otros dispositivos de E/S como, por ejemplo, un teclado, un conjunto de botones o un ratón para permitir que un jugador juegue a un juego de azar en una máquina de juego.

El dispositivo también puede disponer de una memoria de solo lectura (ROM) como, por ejemplo, una memoria 218 de solo lectura programable y borrable (EEPROM) para almacenar un sistema operativo y al menos un programa software para ejecutar un juego de azar y/o procesar los números aleatorios. El sistema operativo y el software se almacenan típicamente en un dispositivo de almacenamiento masivo de lectura/escritura no volátil; sin embargo, la utilización de una EEPROM 218 asegura la integridad del dispositivo 200. La EEPROM 218 asegura la integridad del dispositivo permitiendo que un usuario pueda verificar fácilmente que los contenidos del dispositivo son auténticos si se sospecha la alteración del dispositivo. Por ejemplo, el software en la EEPROM 218

puede asegurar la integridad de los datos en el almacenamiento 214 de números aleatorios permitiendo únicamente procesos software autorizados con firmas digitales válidas para leer, escribir, modificar y eliminar datos en el
5 almacenamiento 214 de números aleatorios. Si se sospecha la alteración del software en la EEPROM 218, el usuario puede simplemente eliminar la EEPROM 218 del dispositivo 200 y verificar los contenidos. De este modo, como el dispositivo 200 se encuentra asegurado en una carcasa, tal como se
10 describe en detalle más abajo, la alteración puede ser visible únicamente si, por ejemplo, está comprometida la cinta a prueba de alteraciones.

Para llevar a cabo un autotest sobre todo el hardware/software en el dispositivo al inicio se puede
15 utilizar un sistema 224 de entrada salida básico de solo lectura (BIOS). En caso de que falle algún componente en el autotest, en la pantalla 220 se puede mostrar un mensaje para informar al usuario sobre el fallo.

Ahora bien, es conocido que el sistema operativo y/o el
20 programa de software se pueden almacenar en cualquier otro componente. Por ejemplo, cuando el dispositivo 200 se inicia, antes de ejecutar cualquier software, la EEPROM 218 puede contener software que verifique la firma digital de los programas de software, incluyendo el sistema operativo que,
25 en ese caso, se puede almacenar en un dispositivo de almacenamiento masivo. En otro modo de realización, la BIOS 224 se puede utilizar para almacenar el sistema operativo y los programas software.

Se puede acoplar un regulador de corriente tensión al
30 generador 400 de números realmente aleatorios y al procesador 210 a través del conjunto 202 de circuitos principal para

mantener y monitorizar la energía suministrada al generador 400 de números realmente aleatorios. Esto asegura la integridad del generador 400 de números realmente aleatorios.

De acuerdo con un ejemplo de modo de realización, el
5 dispositivo de E/S es un conjunto de botones.

Como otro modo de realización, o además, el dispositivo de E/S es un monitor de pantalla táctil.

Como otro modo de realización, o además, el dispositivo de E/S es una rueda mecánica.

10 De acuerdo con un ejemplo de modo de realización la memoria no volátil es una EEPROM.

De acuerdo con un ejemplo de modo de realización la interfaz de E/S es una de un grupo formado por un transceptor inalámbrico, una tarjeta de red, un bus serie universal
15 (USB), un bus de interconexión de componentes periféricos (PCI), o una combinación de los mismos.

De acuerdo con un ejemplo de modo de realización, para llevar a cabo un autotest del dispositivo se proporciona y se acopla al procesador un sistema de entrada salida básico
20 (BIOS).

De acuerdo con un ejemplo de modo de realización para asegurar el dispositivo se proporciona al menos una puerta, una cerradura, un sensor, una cinta de prueba y combinaciones de los mismos.

25 De acuerdo con un ejemplo de modo de realización la memoria es una memoria de acceso aleatorio (RAM).

De acuerdo con un ejemplo de modo de realización se acopla al procesador una memoria de sólo lectura (ROM) para almacenar al menos un programa software.

De acuerdo con un ejemplo de modo de realización la memoria de solo lectura es una memoria de solo lectura programable (PROM).

De acuerdo con un ejemplo de modo de realización la
5 memoria de solo lectura es una memoria de solo lectura programable borrrable electrónicamente (EEPROM).

De acuerdo con un ejemplo de modo de realización la memoria es una memoria no volátil para almacenar un sistema operativo y al menos un programa software.

10 La FIG. 3 muestra un diagrama del sistema de un ordenador 84 utilizado en una máquina de juego de acuerdo con otro ejemplo de modo de realización de la invención. El ordenador 84 incluye una placa base 86, una memoria 88 de programa que es un medio legible por un ordenador, un
15 procesador principal 90 y una RAM 92 conectados mediante una comunicación funcional. El ordenador 84 dispone de un controlador 94 de entrada salida E/S. El controlador 94 de E/S se comunica con un panel 96 de control de interfaces de usuario, un circuito 98 controlador de la interfaz de
20 pantalla, una unidad 100 de pantalla, un monedero 102, un billeteero 104, un lector 106 de tarjetas, una impresora/un lector 108 de tickets, y un circuito 110 de sonido. El circuito 110 de sonido se encuentra en comunicación funcional con los altavoces 112.

25 Un generador 400 de números realmente aleatorios de acuerdo con la presente invención que se muestra en la Fig. 4 con más detalle se encuentra acoplado funcionalmente al procesador principal 90 y a la RAM 92.

El monedero 102 y el billeteero 104 aceptan dinero y
30 comunican la cantidad aceptada al controlador 94 de E/S. El lector 106 de tarjetas lee tarjetas de crédito, tarjetas de

débito, tarjetas regalo u otras tarjetas que tengan indicadores electrónicos de valor monetario.

El lector 108 de tickets imprime tickets y recibos que muestran las ganancias de un jugador u otros resultados económicos. El lector 108 de tickets también recibe tickets
5 que tengan indicadores de valor monetario como, por ejemplo, un código de barras, que es leído por el lector 108 de tickets.

El circuito 110 de sonido está configurado para
10 proporcionar al usuario una interfaz basada en sonido. Cada movimiento o acción de un usuario puede provocar un sonido en particular, o una orden generada por el ordenador 84. Los altavoces 112 comunican los sonidos al usuario.

La Fig. 4 muestra un dispositivo 400 para generar
15 números realmente aleatorios mediante un proceso de óptica cuántica, comprendiendo el dispositivo 400: una fuente 405 de luz para generar al menos un fotón único dentro de un haz de luz; y al menos dos detectores 410, 415 para que cada uno de ellos detecte fotones únicos 450 dentro del haz
20 proporcionando de este modo señales de detección; y medios 420 de control, en donde cada uno de los detectores 410, 415 para detectar fotones únicos comprende al menos un punto cuántico 430, 435; y en donde los detectores se sitúan en una posición sustancialmente equivalente pero en diferente
25 espacio de probabilidad 470 de detección de fotones únicos en el haz; y en donde los medios 420 de control se proporcionan y adaptan para controlar la generación de una serie de fotones únicos y registrar las señales de detección para generar los números realmente aleatorios 460.

30 El equipo está formado por una fuente de luz de fotones, la cual produce un haz de fotones. El haz ilumina una

disposición de al menos dos detectores de fotón único. Se asocia un valor a cada uno de los detectores de esta disposición. La detección de un fotón en un detector dado producirá un número aleatorio, cuyo valor será el asociado
5 con el detector.

Si la disposición de los detectores está formada por dos detectores de fotón único, el equipo producirá números aleatorios binarios. Un detector estará asociado con un valor "0" y el otro detector con un valor "1".

10 La aleatoriedad del número realmente aleatorio producida de este modo se basa en la dualidad onda-partícula de los fotones. La posición de un fotón en el haz se describe por una función de onda. Esta función se puede utilizar para calcular la probabilidad de detección espacial de un fotón en
15 el haz. Si se colocan varios detectores de fotón único en un plano perpendicular al haz, su probabilidad de detección del fotón respectiva estará asociada al valor que toma la función de onda en su posición.

En este sentido, el término "fotón" se refiere a una
20 unidad de energía electromagnética independientemente de su posición en el espectro, por ejemplo, radiación visible o invisible.

Un método de acuerdo con un ejemplo de modo de realización de la invención puede incluir los siguientes
25 pasos. En un primer paso, se ilumina una disposición de detectores mediante un haz de luz que comprende un fotón único. En un segundo paso, se detecta o no el fotón único utilizando al menos dos detectores de la disposición teniendo cada uno de los detectores un punto cuántico. En un tercer
30 paso, se asocia la detección con valores. En un cuarto paso, los valores detectados generan valores de números aleatorios

iguales a los asociados con el detector. En un quinto paso, se repiten los tres pasos anteriores para producir secuencias de números realmente aleatorios. En un sexto paso, utilizando los medios de la circuitería de control, los números
5 aleatorios asociados con las detecciones se registran en un formato apto para la interfaz con un ordenador u otro dispositivo. El dispositivo puede comprender una memoria de almacenamiento temporal.

En un séptimo paso opcional, las secuencias generadas de
10 este modo se procesan para eliminar un posible sesgo, para producir números en una dimensión diferente, o para ajustar la distribución de probabilidad. En un octavo paso opcional, las secuencias de números aleatorios generadas este modo se ponen en cola para su distribución de forma aleatoria a los
15 receptores como semillas o como claves criptográficas, en un modo seguro.

El valor asociado con cada detector se puede determinar utilizando una función de onda que describa la posición de un fotón en el haz. A continuación, se calcula la probabilidad
20 de detección en el espacio de un fotón en el haz. Si se sitúan varios detectores de fotón único en un plano perpendicular al haz, su probabilidad de detección de fotones respectiva está asociada con el valor que toma la función de onda en su posición.

25 Opcionalmente, a continuación se puede procesar la secuencia, por ejemplo, para eliminar un posible sesgo, para producir números en una dimensión diferente, o para ajustar la distribución 36 de probabilidad de un modo, por ejemplo, tal como describe J. von Neumann, "Various techniques used in
30 connection with random digits (Diversas técnicas utilizadas en relación con dígitos aleatorios)", Series de Matemática

Aplicada, 12, 36-38, Oficina Nacional de Estándares de los EE.UU. (1951), cuyo contenido se incorpora en la presente solicitud mediante su referencia.

En otro modo de realización de la invención, la
5 detección de un fotón único en el detector 430 producirá un número realmente aleatorio de valor binario "0", por ejemplo, mientras que la detección de un fotón en el detector 435 producirá un valor binario "1".

Haciendo referencia a la FIG. 4, se muestra una porción
10 de la distribución espacial de la probabilidad 470 de detección de los fotones en un haz, así como la posición de los detectores de fotón único. En función del tipo de fuente de luz utilizada, la forma de la función de distribución espacial puede ser Gaussiana. También son apropiadas otras
15 formas. Si los detectores 410, 415 están situados de forma apropiada en el haz, se puede observar que la probabilidad de detección de un fotón puede ser idéntica para cada detector. Una posición apropiada es, por ejemplo, cerca del centro del haz. La aleatoriedad de los números realmente aleatorios
20 producidos de este modo se basa en la distribución espacial transversal de la probabilidad de detección de un fotón en el haz.

Mediante la repetición de estos pasos, se pueden producir secuencias de números realmente aleatorios. Pasos
25 posteriores procesan la secuencia para, por ejemplo, eliminar un posible sesgo, combinar números aleatorios para producir números en una dimensión diferente, o ajustar la distribución de probabilidad, tal como describe J. von Neumann, "Various techniques used in connection with random digits", citado más
30 arriba.

El equipo es capaz de generar números aleatorios "X-narios", donde X es el número de detectores utilizado en la disposición y representa el número de dimensiones que tiene cada número aleatorio. En dicho caso, el número aleatorio X-nario representa los X bits en un sistema de X dimensiones. Por ejemplo, los símbolos en un sistema binario puede únicamente tener dos significados: tradicionalmente denominados como "on (encendido)" u "off (apagado)". De este modo, un sistema binario es un sistema X-nario en el que X=2.

10 Por ejemplo, cuando la disposición de detectores está formada por dos detectores de fotón único, los números realmente aleatorios producidos son números binarios. Esta disposición de detectores también puede comprender más de dos detectores de fotón único. En un modo de realización se pueden asociar

15 cuatro detectores con valores de 0 a 3 y producir números realmente aleatorios de dimensión 4.

En otro ejemplo, en el sistema decimal, cada dígito puede tener hasta 10 significados, esto es, los números de 0 a 9. En beneficio de la simplicidad, nos referiremos a este

20 sistema como "decimal", un sistema X-nario en el que X=10.

Otra posibilidad es también agrupar los cuatro detectores del conjunto en dos parejas de dos detectores, produciendo cada pareja un número binario.

La disposición de detectores se puede situar perpendicularmente al haz. El plano de la disposición de

25 detectores también puede formar un ángulo α distinto de 90 grados con respecto a la dirección de propagación del haz.

La disposición de detectores se puede reemplazar por guía ondas como, por ejemplo, fibras ópticas (fibra óptica)

30 que guíe la luz hacia los detectores de fotón único.

De acuerdo con un modo de realización, la presente invención proporciona un detector de fotones tal como se muestra en la Fig. 5. Por lo tanto lo que se muestra es una estructura de capas de semiconductor para un detector de fotón único. Se forma una capa 503 de barrera absorbente sobre una superficie superior de un sustrato p+ 505. A continuación se forma una capa 507 de puntos cuánticos sobre una superficie superior de la capa absorbente. Se forma una primera capa 509 de barrera sobre una capa superior de la capa 507 de puntos. Se forma una capa capaz de soportar un gas 511 de electrones en dos dimensiones sobre la capa superior de la 509 de barrera. A continuación se forma una capa 513 superior de barrera sobre la superficie superior de la capa 511 2DEG. La capa de barrera superior es una capa de barrera dopada de modulación que comprende una capa 515 de barrera sin dopar formada superpuesta a la capa 511 de barrera 2DEG y una capa 517 de barrera dopada formada superpuesta a la capa 515 de barrera sin dopar. La estructura está revestida por una capa 519 de recubrimiento. Sobre la capa de recubrimiento se forma una entrada frontal 521. Esta entrada tiene que ser capaz de dejar pasar radiación de ciertas longitudes de onda. Típicamente, la entrada está formada por una capa delgada de NiCr con un espesor de aproximadamente 8 nm. La entrada también puede proporcionarse mediante una capa de semiconductor dopado. A continuación se forma un contacto 523 en la entrada posterior sobre la capa 505 de buffer/sustrato p+. La entrada posterior p+ 505 y la entrada frontal 521 sirven como medio para aplicar un campo eléctrico. En el 2DEG 511 se forman de forma convencional un contacto óhmico 525 de fuente y un contacto óhmico 527 de sumidero. La entrada posterior 505 y la entrada frontal 521

de la entrada pueden estar polarizadas con respecto a un contacto óhmico 527 en el 2DEG.

El detector está configurado para detectar un fotón único, comprendiendo el detector una primera y una segunda
5 capas activas separadas por una primera capa de barrera, y medios de detección para detectar un cambio en una característica de la primera capa activa, en donde la primera capa activa es una capa de pozos cuánticos capaz de soportar un gas portador en dos dimensiones y la segunda capa activa
10 comprende al menos un punto cuántico; el dispositivo comprende, además, medios para separar un par electrón-hueco foto-excitado.

Preferiblemente los medios para separar un par electrón-hueco se proporcionaran para aplicar un campo eléctrico
15 normal a las capas activas. Sin embargo, el dispositivo puede estar fabricado de modo que el campo interno del dispositivo permita la separación de los pares electrón-hueco foto-excitados.

El dispositivo es capaz de detectar un fotón único. Esto
20 es así porque la iluminación óptica del dispositivo da como resultado un cambio en la ocupación de carga de los puntos cuánticos y esto, a su vez induce un cambio en una característica de transporte u óptica de la primera capa activa.

25 La absorción de un fotón único por parte del dispositivo provoca un cambio en la ocupación de un punto cuántico por parte de una portadora y esto a su vez induce un cambio en una característica de transporte u óptica de la primera capa activa. Un fotón único incidente sobre el dispositivo foto
30 excitará un par electrón-hueco dentro del dispositivo. Uno de estos portadores foto-excitados es interceptado por un punto

cuántico e induce un cambio en una característica de la primera capa activa. Por simplicidad, se asumirá que dentro del punto cuántico es interceptado el hueco foto- excitado. Sin embargo, aquellos experimentados en la técnica observarán
5 que el electrón puede ser el portador foto-excitado que es interceptado por el punto.

La presente invención está configurada para detectar la presencia de un fotón único bien por el tamaño del dispositivo, por el número total de puntos en la segunda capa
10 activa, por la estructura de la capa del dispositivo o por el mecanismo de detección real del dispositivo.

El documento de patente GB 2 352 087 describe un detector de fotón único semejante que es barato, compacto y mecánicamente robusto. El detector funciona utilizando
15 tensiones estándar (aproximadamente 5V o menores) y puede funcionar en una temperatura baja o ambiente. Por la presente se incorpora mediante referencia la descripción completa de GB 2 352 087, en particular para una información más detallada de la estructura física y funcionamiento del
20 detector de fotón único.

El detector de fotón único descrito en GB 2 352 087 comprende una primera y segunda capas activas separadas por una primera capa de barrera. La primera capa activa es una capa de pozo cuántico capaz de soportar un gas portador en
25 dos dimensiones y la segunda capa activa comprende al menos un punto cuántico. El dispositivo es capaz de detectar un fotón único debido a que la iluminación óptica del dispositivo da lugar a un cambio en la ocupación de carga del punto cuántico o los puntos cuánticos y esto a su vez induce
30 un cambio en las características de transporte u ópticas de la primera capa activa.

Los medios para aplicar campos eléctricos también pueden comprender un terminal de tipo p y un terminal de tipo n situados en lados opuestos de la primera y la segunda capas activas. En otras palabras, la estructura se encuentra
5 emparejada entre capas dopadas de tipo p y n.

El detector comprende, preferiblemente, un recubrimiento antirreflectante establecido sobre la superficie del dispositivo que se va a iluminar.

El espectro de energía de los puntos cuánticos depende
10 de su tamaño, forma y entorno local. Por lo tanto, diferentes puntos cuánticos poseen diferentes energías de estado básicas y diferentes energías de transición óptica. El dispositivo puede comprender puntos cuánticos de diferentes tamaños que necesitan radiación de diferentes frecuencias para excitar
15 por resonancia un par electrón-hueco.

Un método conveniente para formar una capa de puntos cuánticos es la utilización del modo de crecimiento de Stranski-Krastanow en donde una primera capa se crece sobre una capa con una constante de estructura diferente que la de
20 la primera capa. La primera capa continúa mediante crecimientos de islas tridimensionales y se pueden producir pequeños puntos cuánticos que típicamente tienen unas dimensiones laterales de menos de 50 nm. Un sistema de material preferible para producir este dispositivo utiliza el
25 crecimiento de puntos cuánticos de InAs, InGaAs o InAlAs con barreras de GaAs o (AlGa)As.

El dispositivo se puede formar de tal modo que la capa 2DEG crece antes que la capa de puntos cuánticos. Sin embargo, el orden se puede invertir, esto es, la capa 2DEG
30 formada superpuesta a la capa de puntos. Se pueden utilizar

otros sistemas de estructuras asimétricas como, por ejemplo, InGaN o AlGaN.

Otro posible sistema para producir los puntos utiliza heteroestructuras de SiGe deformadas.

5 El dispositivo también puede estar formado convenientemente de silicio. Aquí, los puntos estarían formados por una capa amorfa de silicio que forma puntos después de endurecer por calor a 800°. Una persona experimentada en la técnica también observará que el germanio
10 podría también proporcionar otro posible material para fabricar el dispositivo.

La detección de fotones únicos también se mejora si el dispositivo comprende, además, una capa de absorción. Una capa de absorción semejante puede ser una capa relativamente
15 gruesa, por ejemplo mayor de 100 nm, la cual forma una capa de barrera a los puntos cuánticos. Los fotones son absorbidos dentro de la capa de absorción, creando pares electrón-hueco dentro de la capa de absorción. Un campo eléctrico aplicado, o un campo eléctrico interno, dentro de la capa de absorción
20 separa los electrones y los huecos que son arrastrados por el campo en direcciones opuestas.

Una polaridad de la portadora es arrastrada a la capa de puntos cuánticos. En general, la capa de absorción se proporcionaría fuera de la región activa del dispositivo,
25 esto es, la capa de absorción no se situaría entre la primera y segunda capas activas. Dicho dispositivo, en general, también comprenderá un sustrato semiconductor.

El detector de fotones de la presente invención no se encuentra limitado a un dispositivo que disponga de
30 únicamente una capa única de puntos. Se pueden proporcionar dos o más capas de puntos para capturar la carga con el fin

de repercutir sobre la conductividad de la primera capa activa. Alternativamente, un detector puede comprender una pluralidad de primeras y segundas capas separadas por una barrera. Este dispositivo también se puede considerar como
5 una pluralidad de detectores de fotones dispuestos uno encima de otro.

Una disposición de detectores de fotones también se puede fabricar comprendiendo una pluralidad de puntos, comprendiendo cada punto un detector de fotones tal como se
10 ha descrito anteriormente más arriba en la presente solicitud. Una disposición de detectores de fotones semejante se puede proporcionar con una malla de líneas de bits y líneas de palabras, en donde cada punto es direccionable aplicando una tensión apropiada a una línea de palabras y/o a
15 una línea de bits.

Preferiblemente, las líneas de bits y las líneas de palabras están configuradas para aplicar una señal de control a los medios para separar un par electrón-hueco foto-excitado.

20 Por ejemplo, si la pluralidad de puntos cuánticos son InAs (o AlInAs) y la primera capa activa es InGaAs (o GaAs), la capa de túnel de barrera podría ser AlAs o Al(x)Ga(1-x)As (o GaAs) con una anchura de entre 10 nm y 500 nm. Más preferiblemente entre 10 nm y 200 nm.

25 Un ejemplo particularmente útil de este dispositivo está proporcionado por un sistema In(y)Al(1-y)As/In(x)Ga(1-x)As. Este sistema permite que la primera capa activa se encuentre fabricada con InGaAs y una región de barrera, comprendiendo una capa de InAlAs situada adyacente a la primera capa
30 activa. La región de barrera es preferiblemente la primera capa de barrera. La gran discontinuidad de la banda de

conducción entre el InGaAs y el InAlAs permite que el dispositivo funcione a temperaturas mucho más altas que aquellas de otros sistemas referidos anteriormente en este documento.

5 La discontinuidad de la banda de conducción donde $x=0.53$ e $y=0.52$ se ha medido entre 500 y 550 meV. El sistema también tenía las ventajas de que da como resultado una baja altura de barrera de Schottky y una movilidad alta.

Tal como se ha explicado anteriormente, el dispositivo
10 comprende, preferiblemente una capa de absorción. Esta capa de absorción se proporciona típicamente como una de las capas de barrera y se proporciona, preferiblemente, fuera de la región activa del dispositivo, esto es, no se situaría entre la primera y segunda capas activas. En una configuración
15 particularmente preferida, la capa de absorción se proporciona en el lado opuesto de la segunda capa activa con respecto a la primera capa activa e incluso más preferiblemente en contacto con la segunda capa activa.

Los fotones únicos se pueden detectar midiendo la
20 corriente a través de la primera capa activa. En general, un fotón único absorbido por el detector provocará un aumento discreto en la corriente que atraviesa la primera capa activa, aunque se debe observar que en algunas configuraciones del detector también se puede observar una
25 disminución discreta. También se pueden medir otros parámetros de la primera capa activa, por ejemplo, la corriente se puede medir en forma de conductividad. También se puede medir la resistividad o la tensión de un lado a otro de la primera capa activa. Independientemente del parámetro
30 que se mida, se observaría un aumento o disminución discretos

en la señal eléctrica de salida cuando el detector absorbe los fotones.

Las medidas de la corriente del detector se pueden basar en un dispositivo de circuito descrito en el documento
5 patente de los EE.UU. 7,199,372, cuya descripción se incorpora por completo en este documento. Así pues, se proporciona un dispositivo de circuito para adaptar la salida de un detector de fotón único, teniendo la salida de dicho detector una señal eléctrica de salida escalonada con
10 respecto al tiempo, comprendiendo el circuito un amplificador paso banda, teniendo dicho amplificador paso banda su punto de rotura de 3 dB superior igual o menor que lo inverso de la duración esperada del paso de aumento o disminución inducido por el fotón de dicha salida del detector.

15 La utilización de dicho amplificador paso banda permite la conversión de los pasos del detector de salida en pulsos que se pueden contar mediante cuenta electrónica al mismo tiempo que se sigue minimizando el ruido provocado por el sistema. Son de interés primordial los flancos de subida de
20 los pasos de la señal de corriente. El amplificador transforma estos pasos en pulsos.

Sin embargo, aquellos experimentados en la técnica apreciarán que también se podrían utilizar cambios de tensión entre ambos extremos de la primera capa activa. También se
25 supondrá que el detector está configurado de modo que la corriente aumenta cuando el detector absorbe los fotones.

Aunque exista un cambio apreciable en la corriente del dispositivo cuando se absorbe un fotón único, el cambio puede ser muy pequeño, típicamente aproximadamente 2 nanoamperios
30 (nA).

De acuerdo con otro modo de realización preferido de generador de números realmente aleatorios la fuente de luz para generar el fotón único está basada en una estructura de punto cuántico. Más en particular, el generador de fotón
5 único puede comprender: una parte de generación de excitones que incluye en la misma un punto cuántico que tiene una estructura de banda para contener un solo excitón; una parte de excitación que genera una pluralidad de excitones, incluyendo dicho excitón único, en dicha parte de generación
10 de excitones; una parte de control de recombinación que controla el tiempo de recombinación de dicho excitón único en dicha parte de generación de excitones; en donde dicha parte de control de recombinación, después de la generación de dicha pluralidad de excitones, provoca la recombinación de la
15 pluralidad de excitones excepto el excitón único en dicha parte de generación de excitones y, posteriormente, cambia dicha estructura de banda para provocar la recombinación de dicho excitón único en dicha parte de generación de excitones.

20 Como otro modo de realización, o además, dicha parte de generación de excitones incluye una heterounión de tipo II en dicho punto cuántico.

Como otro modo de realización, o además, dicho punto cuántico cambia continuamente su composición desde un lado de
25 dicho punto cuántico a otro lado de dicho punto cuántico.

Como otro modo de realización, o además, dicho punto cuántico está formado por un punto cuántico crecido mediante un proceso de crecimiento del modo S-K.

30 Como otro modo de realización, o además, dicho punto cuántico está formado a partir de una laminación de una capa de InAs y una capa de GaSb emparedadas entre un par de capas

de AlAs, cambiando dicha capa de InAs continuamente su composición hacia dicha capa de GaSb.

Como otro modo de realización, o además, dicha parte de control de recombinación comprende un electrodo proporcionado en dicha parte de generación de excitones, una fuente de
5 tensión aplicando una tensión de polarización a dicho electrodo, y un circuito de conmutación controlando la aplicación de dicha tensión de polarización desde la fuente de tensión a dicho electrodo con un intervalo mayor que un
10 ciclo de vida de la recombinación de una molécula de excitón en donde la molécula de excitón se excita en la parte de generación de excitones al mismo tiempo que dicha pluralidad de excitones.

Como otro modo de realización, o además, el generador de
15 fotones únicos puede comprender, además: un miembro de la entrada óptica proporcionado en una ruta de un fotón único, estando formado el fotón único como resultado de la recombinación de dicho excitón único.

Como otro modo de realización, o además, dicho miembro
20 de la entrada óptica está controlado mediante dicha parte de control de recombinación y pasa dicho fotón único sincronizado con la recombinación de dicho excitón único.

El documento de patente US7492901 describe un dispositivo semejante generador de fotones únicos, cuya
25 descripción se incorpora adjunta por completo.

De acuerdo con un ejemplo de modo de realización se proporciona un método para generar una pluralidad de números aleatorios en una máquina de juego, que comprende: generar la pluralidad de números aleatorios a partir de un generador de
30 números realmente aleatorios; compartir al menos una clave de cifrado con un servidor de juego remoto; recibir una petición

desde el servidor de juego remoto de al menos un conjunto de números aleatorios; recuperar el al menos un conjunto de números aleatorios desde una primera memoria; cifrar el al menos un conjunto de números aleatorios; y transmitir al
5 servidor de juego remoto el conjunto cifrado de números aleatorios.

Como otro modo de realización del método, se proporciona el paso de almacenar una copia del conjunto de números aleatorios transmitidos en una segunda memoria.

10 Como otro modo de realización del método, el paso de compartir comprende, además, crear la al menos una clave de cifrado a partir de una pluralidad de números aleatorios.

Como otro modo de realización del método, la al menos una clave de cifrado es una clave simétrica.

15 Como otro modo de realización del método, la al menos una clave de cifrado es un par de clave pública y privada.

Como otro modo de realización del método, dicha compartición comprende, además, generar una petición de certificado para una autoridad de certificación para la
20 autorización del uso de la al menos una clave de cifrado.

Como otro modo de realización del método, se proporciona el paso de recibir un certificado desde la autoridad de certificación.

Como otro modo de realización del método, la transmisión
25 comprende, además, cifrar el al menos un conjunto de números aleatorios por privacidad.

Como otro modo de realización del método, el cifrado comprende, además, firmar digitalmente el al menos un conjunto de números aleatorios.

30 Como otro modo de realización del método, el servidor de juego remoto es la máquina de juego.

Como otro modo de realización del método, se proporciona el paso de recibir una petición para validar y auditar el conjunto de números aleatorios transmitido.

5 Como otro modo de realización del método, se proporciona el paso para contrastar el conjunto de números aleatorios con la copia almacenada en la segunda memoria.

Como otro modo de realización del método, la generación comprende, además, comprobar la pluralidad de números aleatorios para asegurar la aleatoriedad.

10 Como otro modo de realización del método, se proporciona el paso de generación de un juego de azar sobre la máquina de juego con el conjunto de números aleatorios transmitido.

De acuerdo con un ejemplo de modo de realización se proporciona un método para generar una pluralidad de números aleatorios en una máquina de juego que comprende: generar una pluralidad de números aleatorios a partir de un generador de números realmente aleatorios; eliminar el sesgo de la pluralidad de números aleatorios; comprobar la aleatoriedad de la pluralidad de números aleatorios; y almacenar en una memoria la pluralidad de números aleatorios.

15

20

Como otro modo de realización del método, la eliminación comprende, además, los pasos del método: a) emparejar la pluralidad de números aleatorios; b) eliminar al menos un par con numeración común; c) asignar un valor a los pares restantes; y d) separar la pluralidad de bits emparejados en al menos un conjunto de números aleatorios.

25

Como otro modo de realización del método, la comprobación comprende, además, aplicar al menos una prueba de aleatoriedad estadística a la pluralidad de números aleatorios.

30

Como otro modo de realización del método, se proporciona el paso de cifrado de la pluralidad de números aleatorios.

Como otro modo de realización del método, se proporciona el paso de firma digital de la pluralidad de números
5 aleatorios con una clave privada generada a partir de la pluralidad de números aleatorios generados por el generador de números realmente aleatorios.

Como otro modo de realización del método, el almacenamiento comprende, además, eliminar conjuntos de
10 números aleatorios antiguos si la memoria está llena.

Como otro modo de realización del método, se proporciona el paso de generación de un juego de azar a jugar sobre la máquina de juego con la pluralidad de números aleatorios.

Interpretación: a menos que el contexto lo requiera de
15 otro modo, a lo largo de la especificación y las reivindicaciones que siguen, la palabra "comprender" y variaciones de la misma como, por ejemplo, "comprende" y "comprendiendo" se deben interpretar en un sentido abierto inclusivo, esto es, "incluyendo, pero no limitar a".

20 La referencia a lo largo de esta especificación a "un modo de realización" se refiere a un aspecto, estructura o característica particular descrita junto con el modo de realización que se incluye en al menos un modo de realización. Por lo tanto, la aparición de la frase "en un
25 modo de realización" en varios sitios a lo largo de esta especificación no se refieren todos necesariamente al mismo modo de realización. Además, los aspectos, estructuras o características particulares se pueden combinar de un modo apropiado en uno o más modos de realización.

30 Tal como se utiliza en esta especificación y en las reivindicaciones adjuntas, las formas singulares "un", "una",

“el” y “la” incluyen sus plurales al menos que el contexto indique claramente lo contrario. También se debe observar que el término “o” se utiliza, en general, en el sentido de incluir “y/o” a menos que el contexto indique claramente lo contrario.

El título y el Resumen de la Divulgación proporcionados en la presente solicitud son únicamente por comodidad y no interpretan el alcance o significado de los modos de realización.

10 Tal como se utiliza en la presente solicitud, la expresión “números realmente aleatorios” indica números aleatorios generados por un proceso físico.

Tal como se utiliza en la presente solicitud, el término “pozo cuántico” se refiere a una estructura de heterounión
15 doble que incluye una capa ultra fina de un material semiconductor emparedado por una primera capa externa de un material semiconductor y una segunda capa externa de un material semiconductor, donde el salto de banda de la capa ultra fina de material semiconductor es menor que el de la
20 primera capa externa de material semiconductor y el de la segunda capa externa de material semiconductor. La estructura emparedada forma pozos de potencial de banda de conducción y banda de valencia dentro de los que los electrones se encuentran confinados en el pozo de potencial de banda de
25 conducción y los huecos se encuentran confinados en el pozo de potencial de banda de valencia, respectivamente. Un pozo cuántico es un pozo de potencial que confina en su interior portadores (electrones, huecos o pares electrón hueco), forzándolos a ocupar una región plana.

30 El término “punto cuántico”, tal como se utiliza en la presente solicitud, se refiere a una estructura de

heterounión que tiene pozos de potencial de modo que los portadores (electrones, huecos o pares electrón hueco) se encuentran confinados en una pequeña región en la totalidad de las tres dimensiones. Este confinamiento provoca niveles de energía cuantizada discreta y la cuantización de la carga en unidades de carga eléctrica elemental, "e". Debido a que el punto cuántico tiene niveles de energía discretos, de forma parecida a un átomo, en ocasiones se denomina "un átomo artificial". Los niveles de energía del punto cuántico se pueden controlar cambiando el tamaño y la forma del punto cuántico, y la profundidad del potencial.

Tal como se utiliza en la presente solicitud, el término "supermallá" se refiere a una estructura de heterounión multicapa de diferentes materiales semiconductores que se alternan entre sí formando múltiples pozos cuánticos en su interior, cuyas barreras de energía entre pozos cuánticos adyacentes son sustancialmente finas de modo que los electrones puedan experimentar fácilmente el efecto túnel (penetrar de forma mecánico-cuántica) las barreras entre los mismos, ampliándose los niveles de energía discretos en bandas muy pequeñas. La estructura de heterounión multicapa tiene un salto de banda de energía que varía con la posición de una forma deseada. Para el movimiento perpendicular a la capa, los niveles de energía permitidos para los electrones en la banda de conducción y los de los huecos en la banda de valencia son discretos y se encuentran bien separados.

Algunas partes de esta descripción detallada se presentan en términos de procedimientos, pasos, bloques lógicos, procesos, y otras representaciones simbólicas de operaciones sobre bits de datos que se pueden llevar a cabo sobre una memoria de ordenador. Cada paso se puede llevar a

cabo mediante hardware, software, firmware (microcódigo) o combinaciones de ellos.

Cualesquiera ejemplos de una base de datos que se proporcionen son por lo tanto ilustrativos de configuraciones para el almacenamiento de la información. De forma parecida, los ejemplos de topología de red son ilustrativos y se pueden utilizar otras tipologías.

Será fácilmente comprensible para alguien con un conocimiento normal en la técnica que los distintos procesos descritos en la presente solicitud se pueden implementar mediante, por ejemplo, ordenadores de propósito general adecuadamente programados, ordenadores de propósito específico y dispositivos de computación. Típicamente un procesador, por ejemplo, uno o más microprocesadores, uno o más microcontroladores, uno o más procesadores de señales digitales, recibirán instrucciones, por ejemplo, desde una memoria o dispositivo semejante, y ejecutará dichas instrucciones, llevando a cabo de este modo uno o más procesos definidos por dichas instrucciones.

Un "procesador" se refiere a uno o más microprocesadores, unidades centrales de procesamiento CPU, dispositivos de computación, microcontroladores, procesadores de señales digitales o dispositivos similares o una combinación de los mismos.

Así pues, una descripción de un proceso es equivalente a la descripción de un equipo para llevar a cabo el proceso. El equipo que lleva a cabo el proceso puede incluir, por ejemplo, un procesador y aquellos dispositivos de entrada y dispositivos de salida que son adecuados para realizar el proceso.

Además, los programas que implementan dichos métodos así como otro tipo de datos se pueden almacenar y transmitir utilizando una variedad de medios, por ejemplo, medios legibles por un ordenador de distintas formas. En algunos
5 modos de realización, se pueden utilizar circuitos cableados o hardware a medida en lugar de, o en combinación con algunas o todas las instrucciones software que pueden implementar los procesos de diversos modos de realización. Así pues, en lugar de únicamente software se pueden utilizar combinaciones de
10 hardware y software.

El término "medio legible por un ordenador" se refiere a cualquier medio, una pluralidad de los mismos, o una combinación de diferentes medios, que participan proporcionando datos, por ejemplo, instrucciones, estructuras
15 de datos que pueden ser leídas por un ordenador, un procesador o un dispositivo similar. Dicho medio puede tener muchas formas, incluyendo pero no limitándose a, medios no volátiles, medios volátiles y medios de transmisión. Los medios no volátiles incluyen, por ejemplo, discos ópticos o
20 magnéticos y otra memoria persistente. Los medios volátiles incluyen memoria dinámica de acceso aleatorio DRAM, que típicamente constituye la memoria principal. Los medios de transmisión incluyen cables coaxiales, hilo de cobre y fibra óptica, incluyendo los cables que comprenden un bus del
25 sistema acoplado al procesador. Los medios de transmisión pueden incluir o transmitir ondas acústicas, ondas de luz y emisiones electromagnéticas como, por ejemplo, aquellas generadas en las comunicaciones de datos de radio frecuencia RF e infrarrojos IR. Formas comunes de medios legibles por un
30 ordenador incluyen, por ejemplo, un disco flexible, un disco duro, una cinta magnética y otro medio magnético, un CD-ROM,

un DVD, cualquier otro medio óptico, tarjetas perforadas, cinta de papel, cualquier otro medio físico con patrones de agujeros, una RAM, una PROM, una EPROM, una FLASH-EPROM, cualquier otro circuito o cartucho de memoria, una onda
5 portadora tal como se describe más abajo, o cualquier otro medio que pueda leer un ordenador.

Para transportar datos, por ejemplo secuencias de instrucciones, a un procesador se pueden involucrar varias formas de medios legibles por un ordenador. Por ejemplo, los
10 datos se pueden i enviar desde la RAM a un procesador; ii transportar sobre un medio de transmisión inalámbrico; iii formatear y/o transmitir de acuerdo con numerosos formatos, estándares o protocolos como, por ejemplo, Ethernet o IEEE 802.3, SAP, ATP, Bluetooth•, y TCP/IP, TDMA, CDMA y 3G; y/o
15 iv cifrar para asegurar la privacidad o evitar el fraude en cualquiera o una variedad de modos bien conocidos en la técnica.

Así pues una descripción de un proceso es equivalente a una descripción de un medio legible por un ordenador que
20 almacena un programa para realizar el proceso. El medio legible por un ordenador puede almacenar cualquier formato apropiado de estos elementos de programa que sea apropiado para llevar a cabo el método.

Otro ejemplo de modo de realización puede ser un
25 dispositivo de almacenamiento de programas legible por un sistema informático, incorporando el dispositivo de almacenamiento de programas un programa de instrucciones ejecutable por el sistema informático para poner en práctica un método para generar una pluralidad de números aleatorios
30 en una máquina de juego que comprende un dispositivo para generar números realmente aleatorios mediante un proceso de

óptica cuántica de acuerdo con la reivindicación 1 ó 2;
comprendiendo el método los siguientes pasos: generar la
pluralidad de números aleatorios a partir del generador de
números realmente aleatorios; compartir al menos una clave de
5 cifrado con un servidor de juego remoto; recibir una petición
desde el servidor de juego remoto de al menos un conjunto de
números aleatorios; recuperar el al menos un conjunto de
números aleatorios desde una primera memoria; cifrar el al
menos un conjunto de números aleatorios; transmitir al
10 servidor de juego remoto el conjunto de números aleatorios
cifrado; y almacenar en una segunda memoria una copia del
conjunto de números aleatorios transmitido.

Otro ejemplo de modo de realización puede ser un
dispositivo de almacenamiento de programas legible por un
15 sistema informático, incorporando el dispositivo de
almacenamiento de programas un programa de instrucciones
ejecutable por el sistema informático para poner en práctica
un método para generar una pluralidad de números aleatorios
en una máquina de juego, comprendiendo el método: generar una
20 pluralidad de números aleatorios desde un generador de
números realmente aleatorios de acuerdo con los modos de
realización anteriores; eliminar un sesgo de la pluralidad de
números aleatorios; comprobar la aleatoriedad de la
pluralidad de números aleatorios; y almacenar en una memoria
25 la pluralidad de números aleatorios.

Así como la descripción de varios pasos en un proceso no
indica que sean necesarios todos los pasos descritos, los
modos de realización de un equipo incluyen un
ordenador/dispositivo de computación utilizable para llevar a
30 cabo parte aunque no necesariamente todo el proceso descrito.

Igualmente, así como la descripción de varios pasos en un proceso no indica que sean necesarios todos los pasos descritos, los modos de realización de un medio legible por un ordenador que almacena un programa o una estructura de
5 datos incluyen un medio legible por un ordenador que almacena un programa que, cuando se ejecuta, puede dar lugar a que un procesador lleve a cabo parte aunque no necesariamente todo el proceso descrito.

Varios modos de realización se pueden configurar para
10 trabajar en un entorno de red incluyendo un ordenador que se encuentra en comunicación, por ejemplo a través de una red de comunicación, con uno o más dispositivos. El ordenador se puede comunicar directa o indirectamente con los dispositivos a través de un medio cableado o inalámbrico, por ejemplo,
15 Internet, LAN, WAN o Ethernet, Red en Anillo, una línea telefónica, una línea de cable, un canal de radio, una línea de comunicaciones ópticas, proveedores comerciales de servicio en línea, sistemas de mensajería electrónica, un enlace de comunicaciones por satélite o una combinación de
20 cualquiera de los anteriores. Cada uno de los dispositivos puede comprender por sí mismo ordenadores u otros dispositivos computacionales como, por ejemplo, aquellos basados en el procesador Intel® Pentium® o Centrino®, que están adaptados para comunicarse con el ordenador. Cualquier
25 número y tipo de dispositivos se puede encontrar en comunicación con el ordenador.

En un modo de realización, la presente invención se puede llevar a la práctica en una red de uno o más dispositivos sin un controlador central. En dicho modo de
30 realización, cualquiera de las funciones descritas en la presente solicitud como realizadas por el ordenador servidor

o los datos descritos como almacenados en el ordenador servidor pueden llevarse a cabo en su lugar o ser almacenados en uno o más de dichos dispositivos.

5 Cuando se describe un proceso, en un modo de realización el proceso puede realizarse sin ninguna intervención del usuario. En otro modo de realización, el proceso incluye alguna intervención humana, por ejemplo, se lleva a cabo un paso mediante o con la asistencia de una persona.

10 Aunque la presente invención se divulga en términos de varios modos de realización específicos, se puede observar que estos modos de realización se presentan únicamente a modo de ejemplo. El alcance de la invención está definido por las reivindicaciones adjuntas.

15 Se hace constar que con relación a esta fecha, el mejor método conocido por la solicitante para llevar a la práctica la citada invención, es el que resulta claro de la presente descripción de la invención.

REIVINDICACIONES

1. Un dispositivo para generar números realmente aleatorios mediante un proceso de óptica cuántica, comprendiendo el dispositivo:

5 una fuente de luz para generar al menos un fotón único dentro de un haz de luz; y

al menos dos detectores para detectar cada uno de ellos fotones únicos dentro del haz proporcionando de este modo señales de detección; y

10 medios de control,

en donde cada uno de los detectores para detectar fotones únicos comprende al menos un punto cuántico; y

en donde los detectores se encuentran situados en una posición espacial transversal equivalente de probabilidad de
15 detección de fotones únicos en el haz; y

en donde los medios de control se proporcionan y adaptan para controlar la generación de una serie de fotones únicos y para registrar las señales del detector para generar los números realmente aleatorios.

20 2. Un dispositivo como el reivindicado en la reivindicación 1, en donde la fuente de luz para generar el fotón único se basa en una estructura de punto cuántico.

3. Un dispositivo como el reivindicado en una de las reivindicaciones anteriores, en donde el punto cuántico
25 comprende una capa capaz de soportar un gas de electrones en dos dimensiones.

4. Un dispositivo como el reivindicado en una de las reivindicaciones anteriores, en donde la iluminación del haz de luz del detector da lugar a un cambio en la ocupación de
30 carga del punto cuántico y a su vez induce un cambio en una característica óptica o de transporte del detector.

5. Un dispositivo como el reivindicado en una de las reivindicaciones anteriores, en donde se sitúan más de dos detectores en una disposición que comprende una pluralidad de pixels (puntos) comprendiendo cada pixel un punto cuántico
5 detector de fotones.

6. Un dispositivo como el reivindicado en la reivindicación anterior, en donde la disposición del detector comprende una malla de líneas de bits y líneas de palabras, en donde cada pixel es direccionable mediante la aplicación
10 de una tensión apropiada a una línea de palabras y/o a una línea de bits.

7. Un dispositivo, que comprende:
un procesador diseñado o configurado para procesar una pluralidad de números aleatorios; y
15 al menos un generador para generar números realmente aleatorios mediante un proceso de óptica cuántica de acuerdo con una de las reivindicaciones anteriores acoplado al procesador; y
una memoria acoplada al procesador para almacenar la pluralidad de números aleatorios; y
20 una interfaz de entrada/salida (E/S) acoplada al procesador para recibir y/o transmitir datos.

8. Un dispositivo de acuerdo con la reivindicación 7, preferiblemente un dispositivo de juego para jugar un
25 juego de azar, que comprende:
una memoria volátil acoplada al procesador para almacenar la pluralidad de números aleatorios; y
una memoria no volátil acoplada al procesador para almacenar al menos un programa software para jugar al juego
30 de azar; y
una pantalla para visualizar el juego de azar.

9. Un método para generar un número aleatorio, comprendiendo el método los pasos de proporcionar una disposición de al menos dos detectores e iluminarla mediante un haz de luz que comprende un fotón único; y

5 detectar el fotón único utilizando al menos dos detectores de la disposición disponiendo cada uno de los detectores de un punto cuántico y estando asociados a unos valores; y

10 generar el número aleatorio en función de los valores asociados al detector que detecta el fotón único.

10. Un método de acuerdo con la reivindicación anterior, que comprende además la repetición de los pasos de la reivindicación 5 para producir secuencias de números realmente aleatorios.

15 11. Un método de acuerdo con la reivindicación anterior, que comprende además utilizar medios de circuitos de control para formatear números aleatorios asociados con las detecciones apropiados para conectarse con un ordenador u otro dispositivo.

20 12. Un método de acuerdo con la reivindicación anterior, que comprende además eliminar un sesgo en las secuencias generadas de este modo para producir números en una dimensión diferente, o ajustar la distribución de probabilidad.

25 13. Un método de acuerdo con la reivindicación anterior, que comprende además encolar secuencias de números aleatorios generados de este modo para su distribución aleatorizada de forma segura a destinatarios como semillas o claves de cifrado.

30 14. Un dispositivo de almacenamiento de programas legible por un sistema informático, incluyendo el dispositivo

de almacenamiento de programas un programa de instrucciones ejecutable por el sistema informático para aplicar un método para generar una pluralidad de números aleatorios en una máquina de juego que comprende un dispositivo para generar
5 números realmente aleatorios mediante un proceso de óptica cuántica de acuerdo con las reivindicaciones 1 a 6; comprendiendo el método los pasos del método: generar la pluralidad de números aleatorios a partir del generador de números realmente aleatorios; compartir al menos una clave de
10 cifrado con un servidor de juego remoto; recibir una petición desde el servidor de juego remoto de al menos un conjunto de números aleatorios; recuperar el al menos un conjunto de números aleatorios desde una primera memoria; cifrar el al menos un conjunto de números aleatorios; transmitir al
15 servidor de juego remoto el conjunto cifrado de números aleatorios; y almacenar en una segunda memoria una copia del conjunto de números aleatorios transmitidos.

15. Un dispositivo de almacenamiento de programas legible por un sistema informático, incluyendo el dispositivo
20 de almacenamiento de programas un programa de instrucciones ejecutable por el sistema informático para aplicar un método para generar una pluralidad de números aleatorios en una máquina de juego, comprendiendo el método: generar una pluralidad de números aleatorios a partir de un generador de
25 números realmente aleatorios de acuerdo con las reivindicaciones 1 a 6; eliminar un sesgo de la pluralidad de números aleatorios; comprobar la aleatoriedad de la pluralidad de números aleatorios; y almacenar en una memoria la pluralidad de números aleatorios.

RESUMEN

Un dispositivo para generar números realmente aleatorios mediante un proceso de óptica cuántica, comprendiendo el dispositivo: una fuente de luz para generar al menos un fotón
5 único dentro de un haz de luz; y al menos dos detectores para detectar cada uno de ellos fotones únicos dentro del haz proporcionando de este modo señales del detector; y medios de control; en donde cada uno de los detectores para detectar fotones únicos comprende al menos un punto cuántico; y en
10 donde los detectores se sitúan en una posición espacial sustancialmente equivalente de probabilidad de detección de los fotones únicos en el haz; y en donde los medios de control se proporcionan y adaptan para controlar la generación de una serie de fotones únicos y para registrar
15 las señales del detector para generar valores de números realmente aleatorios.

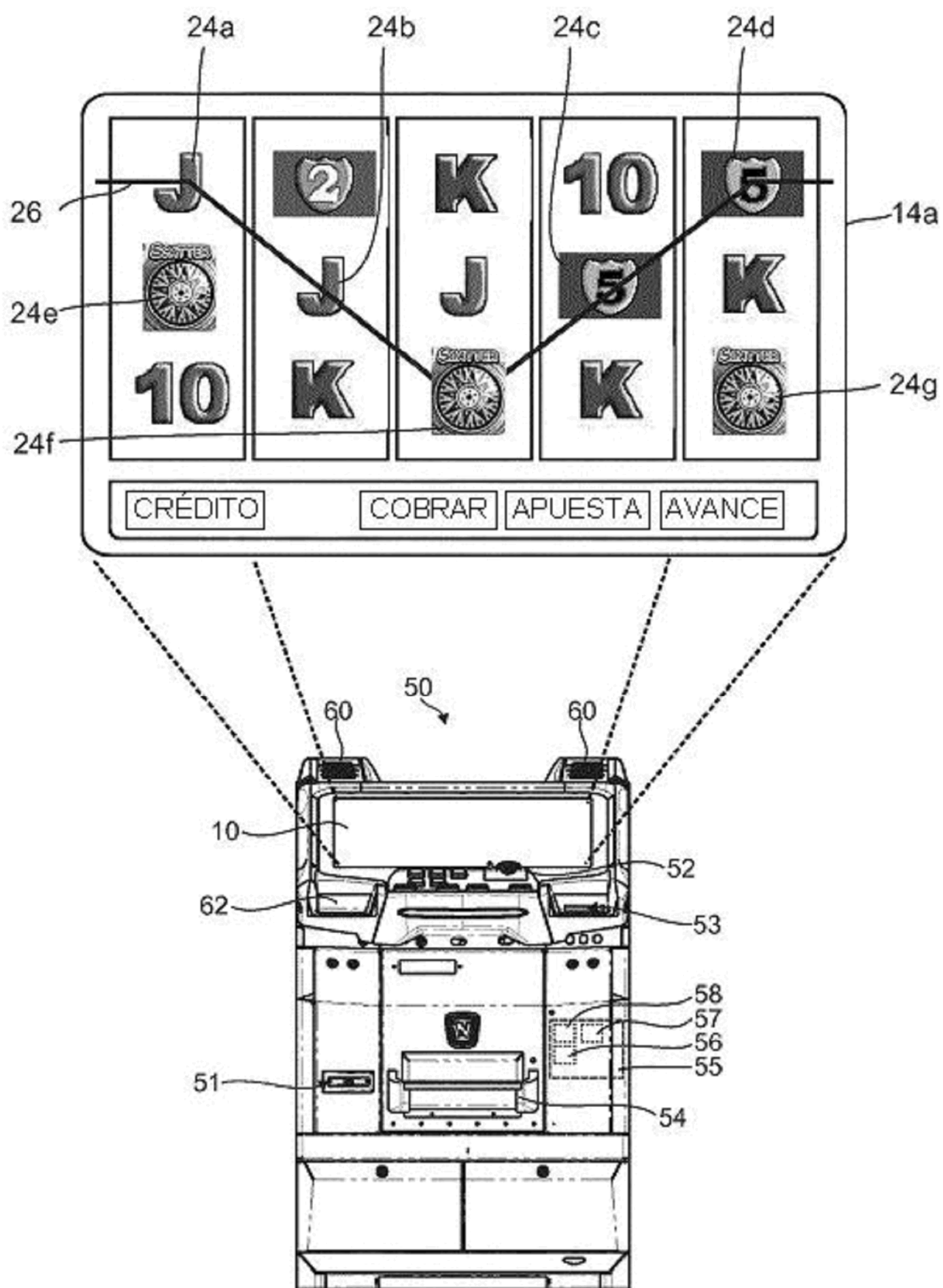


FIG. 1

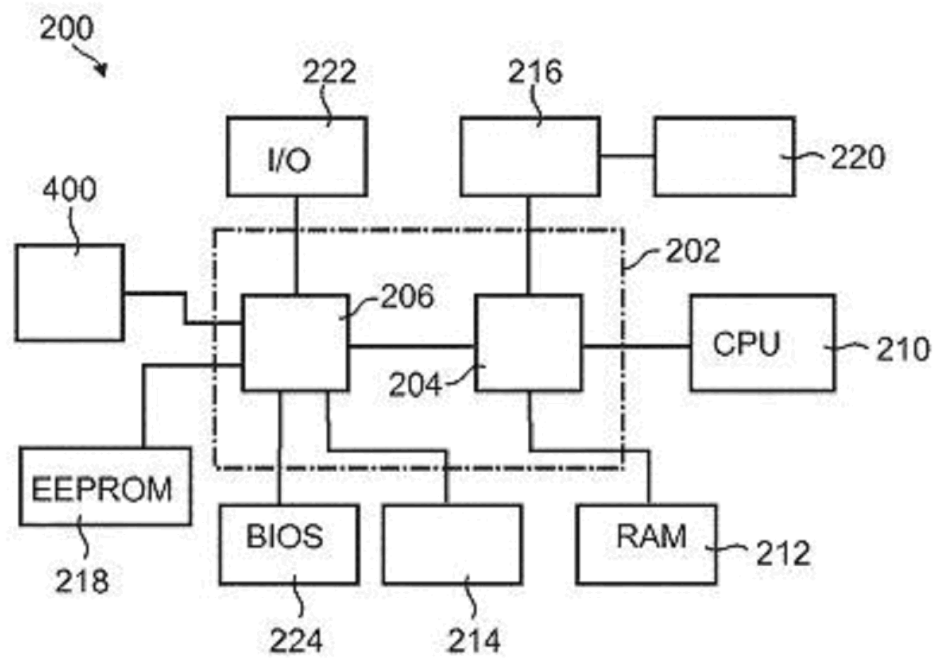


FIG. 2

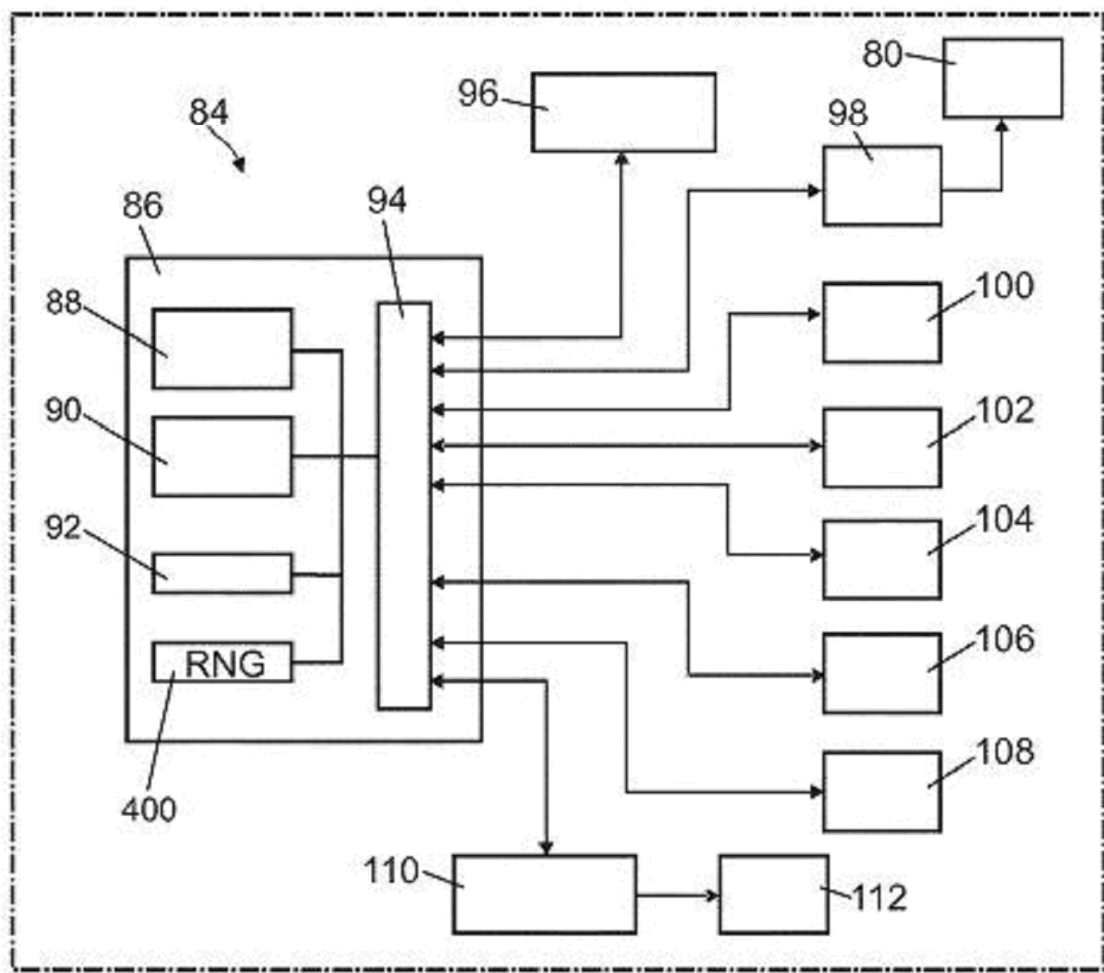


FIG. 3

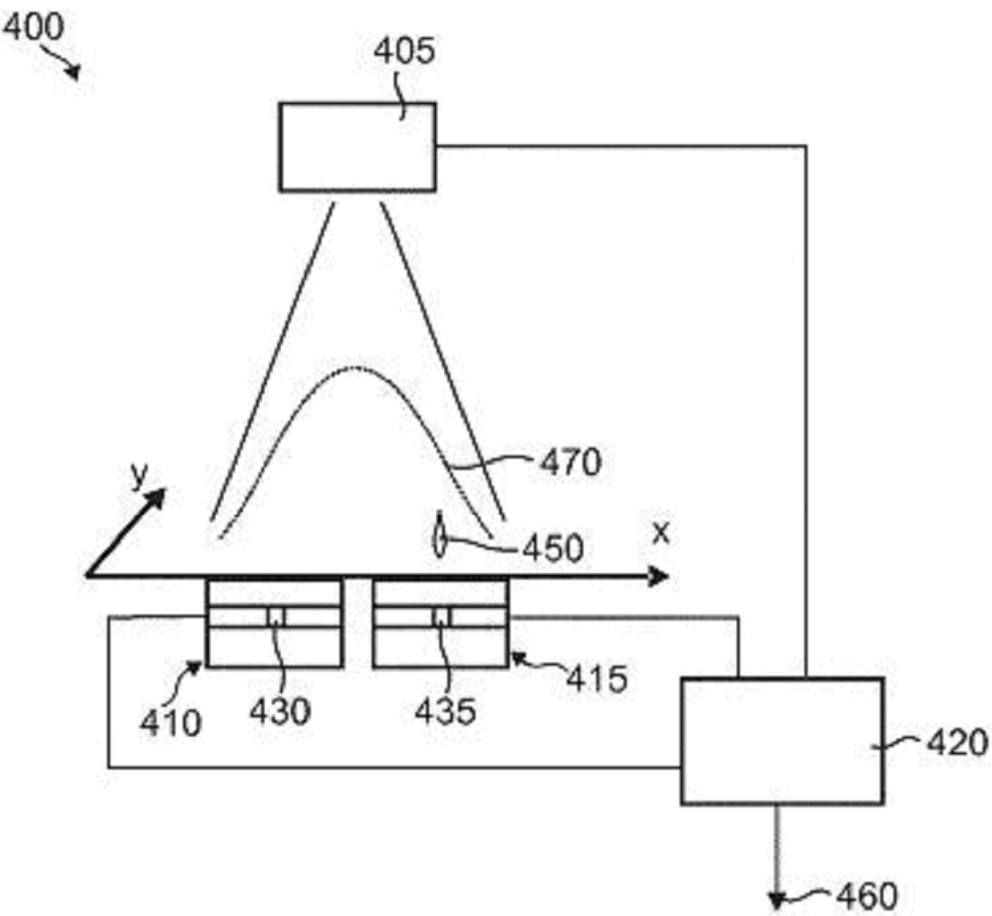


FIG. 4

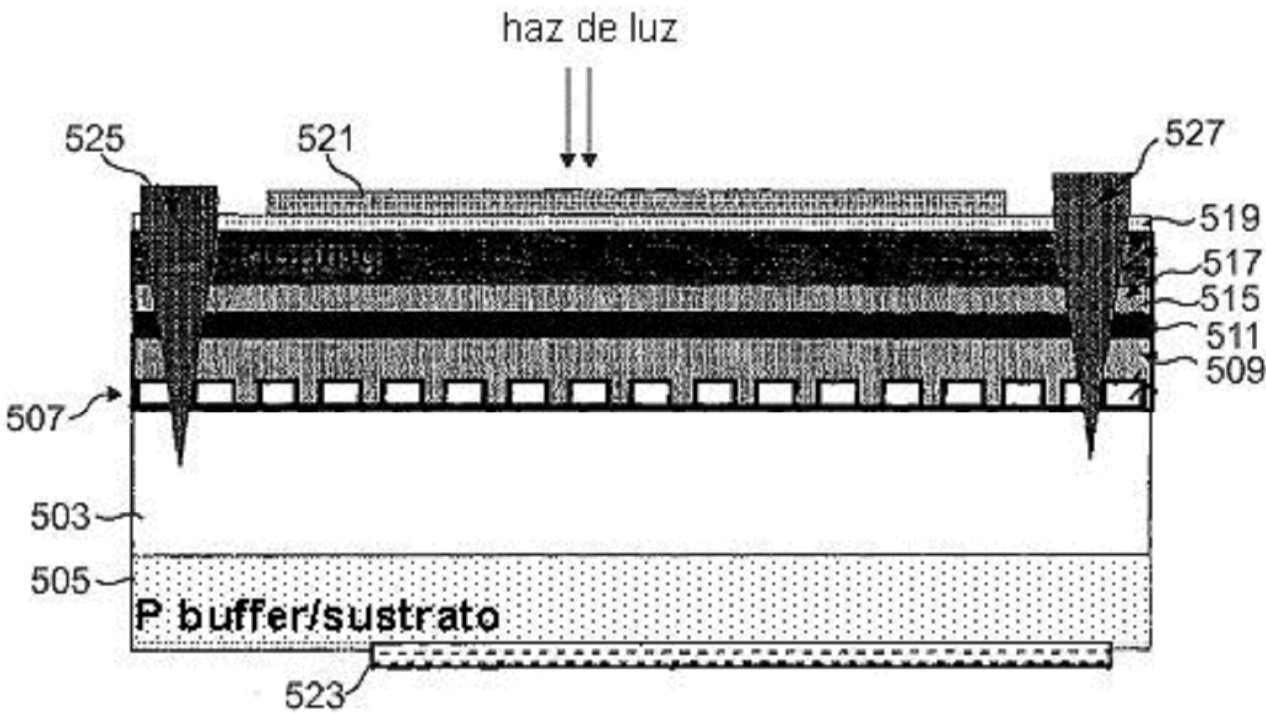


FIG. 5