(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 999 676**

(51) Int. Cl.:

G09C 1/00 (2006.01)
H04L 9/08 (2006.01)
H04L 9/06 (2006.01)
G06F 21/10 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.06.2018 PCT/US2018/036837**

(87) Fecha y número de publicación internacional: **13.12.2018 WO18227174**

(96) Fecha de presentación y número de la solicitud europea: **11.06.2018 E 18814346 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2024 EP 3635725**

(54) Título: **Aparato de seguridad de datos con componente analógico**

(30) Prioridad:

09.06.2017 US 201762517533 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2025

(73) Titular/es:

OPE LLC (50.00%)
6245 Old Rangeline Road
Theodore, Alabama 36582, US y
BOGDANOV, ANDREY (50.00%)

(72) Inventor/es:

BOGDANOV, ANDREY;
SMITH, JOSHUA NORMAN y
MCCOLLUM, ROBERT CHAD

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Aparato de seguridad de datos con componente analógico

Referencia cruzada a aplicaciones relacionadas

Esta solicitud reivindica el beneficio de prioridad de la solicitud de patente provisional n.º US-62/517.533 presentada el 9 de junio de 2017. La patente EP 2 230 794 A2 describe sistemas con fines de seguridad que usan funciones que no pueden clonarse físicamente. La patente US-2015/0006570 A1 describe dispositivos para generar una clave derivada de una clave criptográfica usando al menos una función que no puede clonarse físicamente.

Breve descripción de las figuras del dibujo

Los dibujos se incluyen para proporcionar una mejor comprensión de la siguiente descripción, y se incorporan y constituyen una parte de esta especificación. Los dibujos ilustran ejemplos de implementaciones de la descripción y, con la descripción, explican los principios de la descripción.

La figura 1A ilustra una realización ilustrativa del primer subcomponente 105 del componente analógico 100 que muestra una primera capa.

Las figuras 1B, 1C, 1D, 1E, y 1F son secciones transversales del ejemplo ilustrado en la figura 1A.

La figura 2A ilustra una segunda capa de la realización ilustrativa.

Las figuras 2B, 2C, 2D, 2E, y 2F son secciones transversales del ejemplo ilustrado en la figura 2A.

La figura 3A ilustra una tercera capa de la realización ilustrativa.

Las figuras 3B, 3C, 3D, 3E, y 3F son secciones transversales del ejemplo ilustrado en la figura 3A.

La figura 4A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 4B, 4C, 4D, 4E, y 4F son secciones transversales del ejemplo ilustrado en la figura 4A.

La figura 5A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 5B, 5C, 5D, 5E, y 5F son secciones transversales del ejemplo ilustrado en la figura 5A.

La figura 6A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 6B, 6C, 6D, 6E, y 6F son secciones transversales del ejemplo ilustrado en la figura 6A.

La figura 7A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 7B, 7C, 7D, 7E, y 7F son secciones transversales del ejemplo ilustrado en la figura 7A.

La figura 8A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 8B, 8C, 8D, 8E, y 8F son secciones transversales del ejemplo ilustrado en la figura 8A.

La figura 9A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 9B, 9C, 9D, 9E, y 9F son secciones transversales del ejemplo ilustrado en la figura 9A.

La figura 10A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 10B, 10C, 10D, 10E, y 10F son secciones transversales del ejemplo ilustrado en la figura 10A.

La figura 11A ilustra una cuarta capa de la realización ilustrativa.

Las figuras 11B, 11C, 11D, 11E, y 11F son secciones transversales del ejemplo ilustrado en la figura 11A.

La figura 12A ilustra una realización ilustrativa de una vista inferior de un segundo subcomponente 107 del componente analógico 100.

La figura 12B muestra una sección transversal del ejemplo ilustrado en la figura 12A.

La figura 13A muestra una vista superior de una realización ilustrativa de un componente analógico ensamblado 100 que incluye el primer subcomponente 105 y el segundo subcomponente 107.

Las figuras 13B y 13C muestran secciones transversales del ejemplo ilustrado en la figura 13A.

La figura 14A muestra una realización ilustrativa similar a la figura 11F como un componente analógico 100 ensamblado.

La figura 14B muestra una realización ilustrativa similar a la figura 11E como un componente analógico 100 ensamblado.

La figura 15 muestra las líneas 120 de señal de los primeros electrodos para explicar una operación ilustrativa.

La figura 16 muestra las líneas 120 de señal de los primeros electrodos y los primeros electrodos 320 para explicar una operación ilustrativa.

La figura 17 ilustra una vista superior interior de una celda 1600 de cristal líquido según una operación ilustrativa.

La figura 18 ilustra una vista superior interior de una celda 1600 de cristal líquido según otra operación ilustrativa.

La figura 19A ilustra un aparato 2000 de seguridad de datos para realizar una operación de cifrado.

La figura 19B ilustra un aparato 2000 de seguridad de datos para realizar una operación de descifrado.

La figura 20 ilustra la relación entre el sistema 2100 de circuitos de control y el componente analógico 100 en un aparato 2000 de seguridad de datos.

La figura 21 representa el flujo de operaciones en el sistema 2100 de circuitos de control para las operaciones de cifrado según una realización ilustrativa.

La figura 22 representa el flujo de operaciones en el sistema 2100 de circuitos de control para las operaciones de descifrado según una realización ilustrativa.

La figura 23 muestra la estructura general del de cifrado E1 de bloques cifrado E2 de bloques ilustrativo como una red de sustitución-permutación de 16 rondas, y también la variante de .

La figura 24 ilustra la operación de un esquema de cifrado autenticado (AE, en inglés).

La figura 25 ilustra la construcción de una función E_K usando cifrados de bloques según una realización ilustrativa.

La figura 26 ilustra un modo de operación del contador para el cifrado según una realización ilustrativa.

La figura 27 ilustra un modo de operación del código de autenticación de mensajes según una realización ilustrativa.

La figura 28 ilustra un modo de cifrado AEA global según una realización ilustrativa.

Descripción

Un aparato de seguridad de datos incluye un componente analógico. El componente analógico opera internamente con un alto grado de entropía. Este alto grado de entropía reside en las interacciones entre sus componentes internos en respuesta a una señal de accionamiento externa. Las interacciones dentro del componente analógico tienen un nivel de entropía lo suficientemente alto como para hacer que la simulación digital del componente analógico no sea práctica. Debido a que los componentes analógicos descritos a continuación no son prácticos de simular digitalmente, se denominan no clonables digitalmente.

Los componentes analógicos descritos a continuación reciben una entrada y generan una salida basada en la entrada. Si dos componentes analógicos se fabrican de la misma forma, generarán la misma salida en respuesta a entradas idénticas. La forma en que un componente analógico genera salidas a partir de entradas se denomina firma del componente analógico.

Un aparato de seguridad de datos procesa datos cifrando datos de texto sin formato en texto cifrado y/o descifrando datos de texto cifrado en texto sin formato. Parte de la conversión entre texto sin formato y texto cifrado usa el componente analógico. Dado que el componente analógico no puede clonarse digitalmente (es decir, no es práctico simularlo digitalmente), la parte del proceso de conversión que usa el componente analógico requiere la posesión del propio componente analógico o la posesión de otro componente analógico que tenga la misma firma.

La firma de un componente analógico dado o de un conjunto dado de componentes analógicos se modifica, en varias realizaciones ilustrativas, mediante ajustes en el proceso de fabricación. Los ajustes se aplican de forma fácil y económica, como se explica a continuación. La firma, en otras realizaciones ilustrativas, se modifica fuera de la fabricación del componente analógico.

El aparato de seguridad de datos descrito a continuación es un sistema de cifrado y descifrado de rendimiento que es igualmente aplicable a los datos en tránsito como a los datos en reposo.

Los inventores, mediante estudios de simulación, han dado que el descifrado de solamente un ciclo de datos requeriría dos años de procesamiento con un clúster digital de alto rendimiento. El siguiente ciclo de datos requeriría dos años adicionales. Esta es una función del alto nivel de entropía analizado anteriormente y explicado más adelante. Además, no se espera que la computación cuántica reduzca la impracticabilidad de simular digitalmente la función del componente analógico.

El aparato de seguridad de datos generalmente tiene un componente analógico y un componente de accionamiento. El componente analógico se describe primero, y el componente de accionamiento después.

Componente analógico

Las figuras 1A a 18 representan una realización ilustrativa de un componente analógico 100 para usar en un aparato de seguridad de datos. Esta realización ilustrativa es una realización didáctica proporcionada para enseñar los principios del concepto inventivo. A aquellos familiarizados con este campo se les ocurrirán muchas modificaciones, alteraciones, cambios, mejoras, y alternativas, y se considera que todas están dentro del ámbito del concepto inventivo descrito en la presente memoria. Los límites del concepto inventivo se exponen en las reivindicaciones adjuntas. Además, a menos que se indique lo contrario, puede usarse cualquier técnica de fabricación conocida para construir las estructuras mostradas en las figuras 1A a 13C según las características del equipo disponible y los materiales seleccionados.

Las figuras 1A a 1F muestran en parte un aparato denominado en lo sucesivo componente analógico 100. En estos dibujos, el primer subcomponente 105 se muestra construido sobre el primer sustrato 110. El primer sustrato 110 es, en esta realización ilustrativa, un sustrato de silicio sobre aislante. En otras realizaciones ilustrativas, se proporciona una capa dieléctrica antes de añadir cualquier estructura elaborada de material conductor. El primer sustrato 110 incluye varias almohadillas 130 que son conductoras. Algunas de las almohadillas 130 forman parte integral de las líneas 120 de señal de los primeros electrodos, que también son conductoras. Estos dibujos muestran dieciséis de las líneas 120 de señal de los primeros electrodos. En otras realizaciones ilustrativas, el número de las líneas 120 de señal de los primeros electrodos es sesenta y cuatro o ciento veintiocho. En la presente memoria, el término “primera” no se usa para implicar ningún orden de fabricación, sino solo para discriminarlas de otras líneas de señal descritas más adelante.

Las figuras 2A a 2F muestran en parte la primera capa dieléctrica 210 sobre la disposición dibujada en las figuras 1A a 1F. Las vías 220 de líneas de señal se rellenan con material conductor para extender las líneas 120 de señal de los primeros electrodos. Las almohadillas 130 se extienden similarmente mediante las extensiones 230 de almohadilla. La realización ilustrativa tiene dieciséis de las vías 220 de líneas de señal, una para cada una de las líneas 120 de señal de los primeros electrodos. La figura 2C muestra que las vías 220 de líneas de señal están en contacto directo con las líneas 120 de señal de los primeros electrodos. Esta disposición no es estrictamente necesaria, y otros, componentes intermedios pueden interponerse.

Las figuras 3A a 3F muestran en parte una tercera capa del primer subcomponente 105 del componente analógico 100. La tercera capa incluye el plano 350 a tierra formado de material conductor, los primeros electrodos 320 formados de material conductor, y la segunda capa dieléctrica 310 formada de material aislante. Algunas de las almohadillas 130, que se extienden por medio de las extensiones 230 de almohadilla, son almohadillas 330 a tierra porque están conectadas eléctricamente al plano 350 a tierra.

En la realización ilustrativa dibujada en la figura 3A, el plano 350 a tierra define un área interior en la que se forman los primeros electrodos 320. En la realización ilustrativa dibujada en la figura 3A, los primeros electrodos 320 están todos formados en un lado del área interior y el otro lado del área interior está libre de electrodos.

La figura 3A también muestra que los primeros electrodos 320 están formados en filas y columnas. La longitud de los primeros electrodos 320 varía en dimensión de una fila a otra, como en la sección transversal dibujada en la figura 3E. El ancho y la profundidad de los primeros electrodos 320 son uniformes de columna a columna, como en la sección transversal dibujada en la figura 3D. Haciendo referencia a la figura 3A, con respecto a cualquiera de los dos electrodos dados en filas diferentes, puede decirse que un primero de los electrodos tiene un primer valor dimensional en una primera dirección y un segundo de los electrodos tiene un segundo valor dimensional en esa misma primera dirección (es decir, en la dirección a lo largo de la sección transversal mostrada en la figura 3E), y el primer valor dimensional es diferente del segundo valor dimensional. En otras palabras, la longitud de los primeros electrodos 320 varía, o el ancho, o la profundidad.

En el ejemplo mostrado en las figuras 3A a 3F, la longitud de los primeros electrodos 320 se duplica con cada fila comenzando en la fila más cercana a la parte inferior de. Otras variaciones dimensionales son posibles y constituyen realizaciones ilustrativas alternativas dentro del concepto inventivo.

En la figura 3C, los primeros electrodos 320 están conectados eléctricamente con las respectivas de las líneas 120 de señal de los primeros electrodos. En la presente memoria, "conectado eléctricamente" significa que la carga eléctrica puede viajar a lo largo de una trayectoria de conductores. En la realización ilustrativa de la figura 3C, la trayectoria de los conductores incluye el material conductor formado dentro de las vías 220 de líneas de señal. La presencia de las vías 220 de línea de señal no es estrictamente necesaria en todas las realizaciones ilustrativas. En otras realizaciones ilustrativas, los primeros electrodos 320 forman parte integral de las líneas 120 de señal de los primeros electrodos. En aun otras realizaciones ilustrativas, los primeros electrodos 320 y las líneas 120 de señal de los primeros electrodos están conectadas eléctricamente mediante capas, líneas, y vías adicionales según los requisitos de manipulación de una implementación dada.

En la figura 3C, las extensiones 230 de almohadilla se forman sobre las extensiones 230 de almohadilla a partir de capas formadas previamente. El lector comprenderá que, en esta realización ilustrativa las almohadillas 130 se construyen con cada capa para facilitar el acceso y las pruebas según se desee. Las extensiones 230 de almohadilla pueden omitirse en las almohadillas 130 particulares cuando no se necesitan.

Las figuras 4A a 4F muestran en parte una cuarta capa del primer subcomponente 105 del componente analógico 100. En esta capa, una primera capa 410 de revestimiento y varios postes 450 del plano a tierra se forman sobre la tercera capa. La figura 4D muestra en sección transversal que los postes 450 del plano a tierra están conectados eléctricamente con el plano 350 a tierra.

Las figuras 4C y 4E muestran que los primeros electrodos 320 están inmediatamente por debajo de la primera capa 410 de revestimiento.

Las figuras 5A a 5F muestran en parte una quinta capa, del primer subcomponente 105 del componente analógico 100, en el que una cantidad de elementos están formados de material de guía de ondas que incluye la guía 561 de ondas de entrada, las guías 564 de ondas de salida y los espaciadores 560 de guía de ondas. El número de guías 564 de ondas de salida en otras realizaciones ilustrativas es dieciséis o más. En la realización ilustrativa de las figuras 5A a 5F, el número de 564 corresponde al número de columnas de los primeros electrodos 320. En la presente memoria, los primeros electrodos 320 están formados en cuatro columnas y hay cuatro de las guías 564 de ondas de salida.

En la figura 5A, la guía 561 de ondas de entrada se coloca a lo largo de un extremo de un área que alojará una celda de cristal líquido que se describirá más adelante. Las guías 564 de ondas de salida están colocadas frente a la guía 561 de ondas de entrada en el otro extremo del área que alojará la celda de cristal líquido. El extremo del área en la que se coloca la guía 561 de ondas de entrada puede denominarse extremo de entrada y el extremo del área en la que se colocan las guías 564 de ondas de salida puede denominarse extremo de salida. La figura 5E muestra una sección transversal del primer subcomponente 105 a través de la guía 561 de ondas de entrada, donde la guía 561 de ondas de entrada está a la izquierda del dibujo. La figura 5F muestra una sección transversal del primer subcomponente 105 a través de una de las guías 564 de ondas de salida hacia el lado derecho del dibujo.

Aunque la figura 5E muestra que uno de los primeros electrodos 320 está parcialmente debajo de la guía 561 de ondas de entrada, otras realizaciones ilustrativas no tienen primeros electrodos 320 debajo de ninguna de las guías de ondas.

El número, la posición, y los tamaños de los espaciadores 560 de guías de ondas pueden variar. Los espaciadores a lo largo de los lados izquierdo y derecho del área que aloja la celda de cristal líquido en esta realización ilustrativa facilitan la formación posterior de las paredes laterales de la celda.

Las figuras 6A a 6F muestran en parte una sexta capa, del primer subcomponente 105 del componente analógico 100, en la que la tercera capa dieléctrica 610 se forma en ciertas partes del primer subcomponente 105 pero no se forma en o se retira de otras partes, y en la que se forman extensiones 650 del poste de plano a tierra. Las cavidades 660 del sensor, como se muestra en las figuras 6A, 6B, y 6F, se forman dentro de la tercera capa dieléctrica 610.

La figura 6F muestra la cavidad ilustrada de las cavidades 660 del sensor posicionada para recibir la salida óptica que pasa a través de la guía ilustrada de las guías 564 de ondas de salida.

Las figuras 7A a 7F muestran en parte una séptima capa del primer subcomponente 105 en la que se forman las líneas 720 de señal del sensor. Las líneas 720 de señal del sensor están conectadas eléctricamente con las respectivas almohadillas 130 a través de las extensiones 230 de almohadilla. Además, una de las extensiones 650 del poste de plano a tierra está construida con una extensión adicional 750 del poste de plano a tierra. La figura 7B muestra que la extensión adicional 750 del poste de plano a tierra eleva este poste del plano a tierra particular más arriba que los de las extensiones 650 del poste de plano a tierra que se muestran en la figura 7D. Este es un detalle de implementación proporcionado para la conexión a tierra conveniente de un conjunto de sensores descrito más adelante. Otras implementaciones están dentro del ámbito del concepto inventivo.

Las figuras 8A a 8F muestran en parte una octava capa, del primer subcomponente 105 del componente analógico 100, en la que se forman una cuarta capa dieléctrica 810 y las vías 820 de la línea de señal del sensor. Las vías 820 de la línea de señal del sensor están llenas de material conductor y extienden las líneas 720 de señal del sensor. La cuarta capa dieléctrica 810 no se forma en o se retira de ciertas partes del primer subcomponente 105.

Las figuras 9A a 9F muestran en parte una novena capa, del primer subcomponente 105 del componente analógico 100, en la que la primera capa 910 de poliimida se forma al menos en el área que alojará la celda de cristal líquido. La primera capa 910 de poliimida no se forma ni se retira de al menos las cavidades 660 del sensor.

Las figuras 10A a 10F muestran en parte una décima capa, del primer subcomponente 105 del componente analógico 100, en la que se proporciona el epoxi conductor 1050 en las extensiones del poste 650 de plano a tierra, y en la que se proporciona un material 1070 de junta cerca de los espaciadores 560 de guía de ondas, la guía 561 de ondas de entrada y las guías 564 de ondas de salida.

Las figuras 11A a 11F muestran en parte una undécima capa, del primer subcomponente 105 del componente analógico 100, en la que se proporciona un conjunto 1160 de sensores sobre las cavidades 660 del sensor. El conjunto 1160 de sensores incluye una carcasa 1161 de sensor y uno o más sensores 1164. La carcasa 1161 de sensor se conecta a tierra a través de la línea 1150 a tierra del conjunto de sensores al plano 350 a tierra por medio de otros conductores, tal como se muestra en la figura 11B.

En las figuras 11A a 11F, cada una de las guías 564 de ondas de salida tiene una correspondiente cavidad 660 de sensor y uno correspondiente de los sensores 1164 posicionado encima de las cavidades 660 de sensor. Las entradas y salidas de los sensores 1164 están conectadas eléctricamente a las líneas 720 de señal del sensor.

Por ejemplo, en la figura 11F, una de las guías 564 de ondas de salida se muestra en sección transversal. Esta guía de ondas de salida está posicionada para recibir de la celda de cristal líquido una entrada óptica. Esta guía de ondas de salida también está posicionada para comunicar una salida óptica a la correspondiente de las cavidades 660 del sensor. El uno correspondiente de los sensores 1164 se posiciona encima de una de las cavidades 660 del sensor y realiza una operación de detección cuyo resultado se emite a través de las líneas 720 de señal del sensor. La guía de ondas de salida comunica la salida óptica de la celda de cristal líquido al sensor.

Las figuras 12A y 12B ilustran un segundo subcomponente 107 del primer sustrato 110. La figura 12B muestra la acumulación de tres capas sobre un segundo sustrato 1510 para lograr el segundo subcomponente 107 dibujado en la figura 12A. Para la primera capa, se forma un segundo electrodo 1420 sobre el segundo sustrato 1510. En esta realización ilustrativa, el segundo electrodo 1420 está formado como solo un electrodo y cubre sustancialmente todo el segundo sustrato 1510.

Para la segunda capa, se forma una segunda capa 1310 de revestimiento sobre el segundo electrodo 1420 excepto en las extensiones 1250 del poste a tierra del segundo electrodo. Las extensiones 1250 del poste a tierra del segundo electrodo están conectadas eléctricamente con el segundo electrodo 1420.

Para la tercera capa, se forma una segunda capa 1210 de poliimida sobre la segunda capa 1310 de revestimiento, excepto que las extensiones 1250 del poste a tierra del segundo electrodo se extienden a través de la segunda capa 1310 de revestimiento.

Las figuras 13A a 13C muestran la combinación del primer subcomponente 105 con el segundo subcomponente 107 para formar el componente analógico 100.

Antes del conjunto del primer subcomponente 105 con el segundo subcomponente 107, las capas de poliimida se someten a una preparación denominada frotación. La capa de poliimida se frota a mano en la realización ilustrativa, pero otros procesos de frotación están dentro del ámbito del concepto inventivo. La frotación imparte una alineación molecular a las capas de poliimida. En una realización ilustrativa alternativa, una o más de las capas de poliimida se frotan de modo que la alineación molecular sea una alineación molecular irregular. En otras palabras, una o ambas de la primera capa 910 de poliimida y la segunda capa 1210 de poliimida se frotan en más de una dirección, lo que aumenta la dificultad para predecir o modelar la función del componente analógico 100.

Como se muestra en la figura 13B, las extensiones 650 del poste de plano a tierra se unen con las extensiones 1250 del poste a tierra del segundo electrodo en virtud del epoxi conductor 1050. Cuando el segundo subcomponente 107 se ajusta al primer subcomponente 105, la segunda capa 1210 de poliimida comprime y deforma el material 1070 de junta. El material 1070 de junta que se ha comprimido y deformado presiona contra los lados de la guía 561 de ondas de entrada, contra los lados de las guías 564 de ondas de salida, y contra un lado de los espaciadores 560 de guía de onda para proporcionar paredes laterales que encierran una cavidad para una celda de cristal líquido.

La cavidad se muestra en la figura 14A y en la figura 14B llenándose con material de cristal líquido para formar la celda 1600 de cristal líquido. En la figura 14A, la cavidad 660 del sensor ilustrada se muestra llena de, por ejemplo aceite óptico para facilitar el transporte de la luz desde una de las guías 564 de onda de salida hasta uno de los sensores 1164.

La inserción del material de cristal líquido en la cavidad se realiza de cualquier modo convencional, por ejemplo usando un vacío inducido a través de un puerto (no ilustrado) que se mantiene abierto para tal fin y luego se cierra permanentemente.

Anteriormente, se señaló que los primeros electrodos 320 están conectados eléctricamente con las respectivas líneas 120 de señal de los primeros electrodos. La figura 14B ilustra que la celda 1600 de cristal líquido está sobre los primeros electrodos 320. Aunque la celda 1600 de cristal líquido está solo parcialmente sobre el extremo izquierdo y el extremo derecho de los primeros electrodos 320 todavía está sobre los primeros electrodos 320.

La figura 14B también muestra un segundo electrodo 1420 sobre la celda 1600 de cristal líquido. El ejemplo mostrado en la figura 14B incluye solo un segundo electrodo que está sobre la totalidad de la celda 1600 de cristal líquido. En otras realizaciones ilustrativas, se proporciona más de un segundo electrodo. Ya sea que se proporcione solo uno o más de un segundo electrodo, los segundos electrodos deben estar opuestos a los primeros electrodos 320 del modo dibujado en la figura 14B. En otras palabras, el primer y segundo electrodos están en lados opuestos de la celda 1600 de cristal líquido, de modo que puede formarse una carga eléctrica entre los primeros electrodos 320 y el segundo electrodo 1420 y provocar que los cristales en el material de cristal líquido cambien de orientación dentro de la celda 1600 de cristal líquido.

El componente analógico 100 se ha enseñado en el contexto de un primer subcomponente 105 y un segundo subcomponente 107. En otras realizaciones ilustrativas el componente analógico 100 se forma con diferentes capas en cada uno de los subcomponentes. En otras realizaciones ilustrativas las capas se combinan y/o reorganizan.

Operación del componente analógico

Durante la operación, se introduce una entrada óptica que es en una realización ilustrativa es una entrada óptica coherente en la guía 561 de ondas de entrada. La guía 561 de ondas de entrada comunica la señal óptica a la celda 1600 de cristal líquido. A medida que se energizan las líneas 120 de señal de los primeros electrodos, las cargas eléctricas entre los primeros electrodos 320 y el segundo electrodo 1420 hacen que los cristales en la celda 1600 de cristal líquido cambien de orientación. El paso de la entrada óptica a través de la celda 1600 de cristal líquido se ve afectado por la orientación de los cristales. Los cristales causan difusión, interferencia constructiva, e interferencia destructiva de una manera impredecible.

Las guías 564 de ondas de salida reciben la salida óptica de la celda 1600 de cristal líquido, sea lo que sea, y la comunican a las cavidades 660 del sensor. La salida variará de una guía de ondas de salida a otra. La salida óptica de la celda 1600 de cristal líquido, transportada a través de las guías 564 de ondas de salida, entra en el aceite óptico en las cavidades 660 del sensor y, a través de este medio, se comunica a los sensores 1164.

De este modo, los sensores 1164 detectan la salida óptica de la celda 1600 de cristal líquido.

La realización ilustrativa dibujada en las figuras 14A y 14B puede modificarse de muchas formas dependiendo del conjunto 1160 de sensores particular. La realización ilustrativa de las figuras 14A y 14B muestra una implementación en la que el conjunto 1160 de sensores se instala como un dispositivo separado, en o cerca del final de la fabricación del componente analógico 100. El resultado de esta implementación es un ángulo entre la salida de las guías 564 de ondas de salida y la entrada a los sensores 1164. El aceite óptico se usa para ayudar a que la salida llegue a los sensores 1164. A aquello familiarizados con este campo se les ocurrirán alternativas tales como el uso de una superficie reflectante, en ángulo dentro de las cavidades 660 del sensor.

En otras realizaciones ilustrativas, los sensores 1164 se fabrican como una estructura integral del componente analógico 100 y están orientados de modo que la salida óptica de la celda 1600 de cristal líquido pase a través de las guías 564 de ondas de salida y directamente a los sensores 1164 sin cambiar de dirección.

En otra realización ilustrativa la salida óptica de la celda 1600 de cristal líquido es transportada por las guías 564 de ondas de salida a una fibra óptica acoplada a tope que, a su vez, proporciona la salida a los sensores 1164.

En otras realizaciones ilustrativas, el conjunto 1160 de sensores está fuera del chip. Tener los sensores 1164 en el chip tiene la ventaja de que el componente analógico 100 es más resistente a la manipulación inversa. La descripción anterior ha explicado, en términos generales, que un aparato que tiene sus primeros electrodos conectados eléctricamente con las respectivas líneas de señal de los primeros electrodos, una celda de cristal líquido sobre los primeros electrodos, uno o más segundos electrodos sobre la celda de cristal líquido y opuestos a los primeros electrodos, una guía de ondas de entrada configurada para comunicar una entrada óptica a la celda de cristal líquido y un sensor configurado para detectar una salida óptica de la celda de cristal líquido. El aparato también tiene una guía de ondas de salida configurada para comunicar la salida óptica de la celda de cristal líquido al sensor.

Como muestra la figura 14B, cada uno de los dibujos de los primeros electrodos 320 tiene un valor dimensional diferente (longitud, en este ejemplo) en una primera dirección (de izquierda a derecha en el dibujo, en este ejemplo). Estas diferencias de dimensión entre los primeros electrodos 320 tienen la ventaja de que la carga proporcionada entre los primeros electrodos 320 y el segundo electrodo 1420, y el efecto correspondiente sobre la orientación de los cristales en la celda 1600 de cristal líquido, es más caótica y, por lo tanto, más resistente al análisis y a la ingeniería inversa.

Con referencia a la figura 3A, la disposición de los primeros electrodos 320 puede considerarse como un aspecto de la firma particular de un componente analógico 100 dado. Dos ejemplos del componente analógico 100 que tienen la misma firma operarán igual, o lo suficientemente parecido como para ser idénticos, para lograr la interoperabilidad para fines de conversión entre texto sin formato y texto cifrado, descrito más adelante. Dos ejemplos del componente analógico 100 cuyas firmas no coincidan no serán interoperables.

El componente analógico 100 descrito a modo de ejemplo simplificado, anteriormente, posee varios aspectos que pueden alterarse fácilmente para lograr diferentes firmas. Como ya se ha mencionado, la disposición de los primeros electrodos 320 es uno de esos aspectos. Para variar este aspecto de la firma de un dispositivo dado, en la producción solo es necesario variar la máscara mediante la cual se proporcionan los primeros electrodos 320. La ubicación, la longitud, el ancho y la forma de unos determinados de los primeros electrodos 320 se varían fácilmente variando la máscara. Otros aspectos que pueden variarse para obtener diferentes características para tales componentes analógicos incluyen variar la frotación de poliimida de la primera capa 910 de poliimida y/o la segunda capa 1210 de poliimida, variar la receta usada para el material con el que se llena la celda 1600 de cristal líquido, variar el material particular usado para construir la guía 561 de ondas de entrada y las guías 564 de ondas de salida.

En varias realizaciones ilustrativas, un controlador de temperatura (no ilustrado) regula la temperatura del material en la celda 1600 de cristal líquido para lograr un funcionamiento constante en una variedad de entornos. Otro aspecto que puede variarse para obtener una firma diferente para un componente analógico 100 es la temperatura a la que se regula la celda 1600 de cristal líquido.

Las combinaciones de los aspectos anteriores varían para lograr conjuntos de uno o más componentes analógicos que sean adecuados para la interoperación, o para lograr un componente analógico que no sea interoperable con otros.

En operación se introduce una entrada óptica constante en la guía 561 de ondas de entrada. La salida de la celda 1600 de cristal líquido se detecta en los sensores 1164. Puede proporcionarse una entrada de componente analógico A_i al componente analógico 100 a través de las líneas 120 de señal de los primeros electrodos. La entrada A_i del componente analógico es una secuencia de valores binarios, o bits.

En la realización ilustrativa mostrada parcialmente en la figura 15, el componente analógico 100 tiene dieciséis de las líneas 120 de señal de los primeros electrodos numeradas individualmente del 120-0 al 120-F. Las señales de estas líneas 120 de señal de los primeros electrodos viajan a los primeros electrodos 320 porque las líneas 120 de señal de los primeros electrodos están conectadas eléctricamente con los respectivos primeros electrodos 320. En la realización ilustrativa mostrada parcialmente en la figura 16, el componente analógico 100 tiene dieciséis primeros electrodos 320. Los primeros electrodos 320 están numerados individualmente del 320-0 al 320-F. La línea 120-0 de señal de los primeros electrodos está conectada eléctricamente al primer electrodo 320-0 y así sucesivamente.

La entrada de componente analógico A_i se introduce en el componente analógico 100 dieciséis bits a la vez en esta realización ilustrativa. Bajo el control de un reloj, por ejemplo, los valores respectivos de los siguientes dieciséis bits de un flujo de bits se usan para accionar las respectivas líneas 120 de señal de los primeros electrodos. Por ejemplo, si el bit 0-ésimo tiene un valor de 1, entonces se activa la línea 120-0 de señal de los primeros electrodos. Por ejemplo, si el 1er bit tiene un valor de 0, entonces la línea 120-1 de señal de los primeros electrodos no se activa, y así sucesivamente a través del F-ésimo bit. La activación de algunas de las líneas 120 de señal de los primeros electrodos. da como resultado la introducción de carga en las correspondientes de los primeros electrodos 320. En cualquier ciclo particular, por lo tanto, algunos de los primeros electrodos 320 se cargan según el valor de los dieciséis bits dados del flujo de bits usado como entrada de componente analógico A_i y algunos otros de los primeros electrodos 320 no están cargados.

Los primeros electrodos 320 están todos opuestos a al menos un segundo electrodo 1420 de modo que cuando aparece carga en uno dado de los primeros electrodos 320, los cristales del material de cristal líquido en la celda 1600 de cristal líquido se ven afectados.

La figura 17 ilustra una realización ilustrativa de un resultado simulado de aplicar "0110000010010000" como dieciséis bits de una entrada de componente analógico *A_i a las líneas 120 de señal de los primeros electrodos*. En la presente memoria, el bit más significativo (a la izquierda) se usa para accionar la línea 120-0 y el bit menos significativo (a la derecha) se usa para accionar 120-F. En este ejemplo, las líneas 120-1, 120-2, 120-8, y 120-B están accionadas. Los electrodos 320-1, 320-2, 320-8, y 320-B correspondientes se energizan, lo que afecta a la orientación de los cristales en la celda 1600 de cristal líquido. En la figura 17, los cristales en la celda 1600 de cristal líquido están representados por prismas cuadrados que se extienden longitudinalmente en una dirección desde la parte superior hasta la parte inferior del dibujo cuando no están perturbados por ninguna carga. En el dibujo, los cristales se realinean en una

dirección que sale de la página cuando una carga los mueve por completo, y adoptan posiciones intermedias cuando hay una carga pero es insuficiente para reorientar completamente los cristales.

La figura 18 es similar a la figura 17, pero los dieciséis bits de la entrada A del componente analógico son "1011110111100111". Los electrodos 320-0, 320-2 a 320-5, 320-7 a 320-A, y 320-D a 320-F están cargados. El área rodeada por una elipse dibujada con una línea discontinua, en este resultado simulado, contiene cristales que se ven afectados por la carga proveniente de los electrodos cercanos 320-0, 320-2, 320-D, y 320-F, aunque estos cristales no estén directamente debajo de ninguno de los primeros electrodos 320. Estos cristales simulados están casi completamente reorientados. Compare ahora el área entre los electrodos 320-5 y 320-6, en la que los cristales entre estos dos electrodos se ven afectados por la carga cercana, pero no hasta el punto de alcanzar una reorientación total.

La luz introducida en la guía 561 de ondas de entrada pasará a las guías 564 de ondas de salida de modo diferente en los ejemplos de la figura 17 y la figura 18, con el resultado de que los valores detectados en los sensores 1164 serán diferentes en cada caso.

Las diferentes longitudes de los primeros electrodos 320 aumentan la entropía de las interacciones internas entre la luz introducida a través de la guía 561 de ondas de entrada y los numerosos cristales de la celda 1600 de cristal líquido.

La formación de los primeros electrodos 320 a lo largo de menos de toda la celda 1600 de cristal líquido (la mitad dibujada en el lado derecho en las figuras 17 y 18) también aumenta la entropía y contribuye a la no clonabilidad digital del componente analógico 100.

La entrada de componente analógico A_i en la realización ilustrativa anterior se toma dieciséis bits a la vez. Cada uno de los cuatro sensores 1164 es lo suficientemente sensible como para detectar dieciséis variaciones en la luz. En otras palabras, cada sensor puede emitir valores que pueden codificarse en cuatro bits. Los cuatro bits codificados a partir de las salidas de cada uno de los cuatro sensores 1164 son dieciséis bits en total. Estos cuatro conjuntos de cuatro bits se concatenan para dar una salida de componente analógico de dieciséis bits A_o.

En el ejemplo anterior, se usó un flujo de bits para accionar las líneas 120 de señal de los primeros electrodos del componente analógico 100. El flujo de bits, tomado dieciséis bits a la vez, es más generalmente una entrada A_i del componente analógico.

En el ejemplo anterior, la salida A_o del componente analógico de dieciséis bits se determinó por lo que los sensores 1164 detectaron después de que los cristales de la celda 1600 de cristal líquido se vieran afectados por la entrada A_i del componente analógico. En otras palabras, la salida A_o del componente analógico se basó en la entrada A_i del componente analógico. Usando un sistema de circuitos de control adecuado, descritos a continuación, es posible obtener repetidamente del componente analógico 100 una salida de componente analógico A_o basada en la entrada de componente analógico A_i, *procesando de este modo un* flujo de bits de longitud arbitraria en porciones de dieciséis bits.

Mientras que la realización ilustrativa anterior usaba dieciséis de las líneas 120 de señal de los primeros electrodos, dieciséis de los primeros electrodos 320, cuatro de las guías 564 de ondas de salida y cuatro de los sensores 1164, estos números se usaron para enseñar al lector el concepto inventivo.

El diseño del componente analógico 100 en otra realización ilustrativa procesa un flujo de bits en porciones de doscientos cincuenta y seis bits usando doscientas cincuenta y seis de las líneas 120 de señal de los primeros electrodos. Este ejemplo se denominará más adelante chip de 256 bits. Cada una de estas líneas 120 de señal de los primeros electrodos está conectada a los correspondientes de los doscientos cincuenta y seis primeros electrodos 320. Estos primeros electrodos 320 están dispuestos en cuatro filas como en la figura 18, pero tienen sesenta y cuatro de los primeros electrodos 320 en cada fila. Este ejemplo de chip de 256 bits tiene sesenta y cuatro guías 564 de ondas de salida, y cada una de estas guías 564 de ondas de salida comunica una salida óptica de la celda 1600 de cristal líquido a los correspondientes de los sesenta y cuatro sensores 1164. Los sensores 1164 emiten valores de cuatro bits que se concatenan para proporcionar una salida de componentes analógicos A_o de doscientos cincuenta y seis bits.

En aun otra realización ilustrativa similar al chip de 256 bits descrito en el párrafo inmediatamente anterior, solo se forman treinta y dos de las guías 564 de ondas de salida y solo se proporcionan treinta y dos de los sensores 1164. Sin embargo, en este ejemplo, cada sensor es lo suficientemente sensible como para emitir valores de ocho bits. Los treinta y dos valores de ocho bits se concatenan para proporcionar una salida de componentes analógicos A_o de doscientos cincuenta y seis bits. En otra realización ilustrativa similar al chip de 256 bits, los primeros electrodos 320 están dispuestos en más o menos filas y columnas. En otras realizaciones ilustrativas, las posiciones de las guías 564 de ondas de salida se establecen para maximizar la entropía. Al lector se le ocurrirán otras variaciones sin apartarse de los conceptos inventivos descritos en esta memoria.

La descripción anterior explica cómo la interconexión entre las líneas 120 de señal de los primeros electrodos y los primeros electrodos 320 determina cuáles de los primeros electrodos 320 se cargan cuando se accionan las líneas 120 de señal de los primeros electrodos. La alteración del patrón de conexión entre las líneas 120 de señal de los primeros electrodos y los primeros electrodos 320 da como resultado una firma diferente de un componente

analógico 100. Por lo tanto, además de las diversas formas en las que puede variarse la formación del componente analógico 100, también puede variarse la formación de las conexiones entre las líneas 120 de señal de los primeros electrodos y los primeros electrodos 320. En una realización ilustrativa, se proporcionan capas de interconexión adicionales para que la conexión entre las líneas 120 de señal de los primeros electrodos y los primeros electrodos 320 pueda variarse convenientemente.

Componente de accionamiento

El componente analógico 100 es útil, por ejemplo, como parte de un aparato 2000 de seguridad de datos mostrado generalmente en las figuras 19A y 19B. En la figura 19A, el aparato 2000 de seguridad de datos recibe un mensaje M de texto sin formato que también puede denominarse datos digitales *M.* El término "texto sin formato", tal como se usa en la presente memoria, no significa que el mensaje *M* de texto sin formato deba representar un mensaje legible por humanos. El mensaje *M* de texto sin formato representa cualquier conjunto de bits antes de cifrarse. El mensaje *M* de texto sin formato en varias realizaciones ilustrativas se cifra previamente mediante algún otro proceso y, en otras realizaciones ilustrativas, son datos no cifrados previamente por otro proceso.

Mediante un proceso de cifrado, el aparato 2000 de seguridad de datos convierte el mensaje *M* de texto sin formato en texto cifrado *C*. En la figura 19B, el aparato de seguridad de datos 2000 recibe el texto cifrado *C.* A través de un proceso de descifrado, el aparato 2000 de seguridad de datos convierte el texto cifrado *C* de nuevo en un mensaje *M* de texto sin formato que coincide con el mensaje *M* de texto sin formato introducido originalmente en la figura 19A.

Las figuras 19A y 19B están muy simplificadas, pero proporcionan una idea general del entorno en el que se usa el componente analógico 100. El aparato 2000 de seguridad de datos mostrado en las figuras 19A y 19B es, en un ejemplo, el mismo aparato 2000 de seguridad de datos pero realiza el cifrado o el descifrado usando al menos un componente analógico 100. En otro ejemplo, el aparato 2000 de seguridad de datos de la figura 19A está separado del aparato 2000 de seguridad de datos en la figura 19B mediante un enlace de comunicación, y en realizaciones ilustrativas, está alejado del aparato 2000 de seguridad de datos de la figura 19B. En este último ejemplo, la firma del aparato 2000 de seguridad de datos en cada una de las figuras 19A y 19B debe coincidir o el mensaje *M* de texto sin formato introducido en la una no coincidirá con el mensaje *M* de texto sin formato emitido por la otra.

La figura 20 ilustra una realización ilustrativa del aparato 2000 de seguridad de datos de la figura 19A con mayor detalle. El aparato 2000 de seguridad de datos incluye un sistema 2100 de circuitos de control y un componente analógico 100. El sistema 2100 de circuitos de control recibe el mensaje *M* de texto sin formato desde el exterior del aparato 2000 de seguridad de datos y envía el texto cifrado *C* al exterior del aparato 2000 de seguridad de datos. Parte del procesamiento del mensaje *M* de texto sin formato en el texto cifrado *C* usa el componente analógico 100.

El sistema 2100 de circuitos de control se implementa como un circuito integrado de aplicación específica (ASIC, en inglés) en una realización ilustrativa.

En otra realización ilustrativa, el sistema 2100 de circuitos de control se implementa como una matriz de puertas programables en campo (FPGA, en inglés). Mientras que un ASIC se configura antes de la fabricación, un FPGA es un circuito integrado que puede configurarse después de la fabricación mediante un lenguaje de descripción de hardware (HDL, en inglés) similar al usado para describir un ASIC.

El HDL define el comportamiento de la FPGA y programa la FPGA para que tenga una estructura que lleve a cabo las funciones previamente definidas. En otras palabras, la estructura de la FPGA está definida por el HDL, lo que convierte a una FPGA programada en un circuito electrónico estructuralmente único en la forma de un ASIC.

La relación entre la estructura de una FPGA y la HDL usada para programarla (y, asimismo, la relación entre la estructura de un ASIC y la HDL usada para definir su fabricación) se reformula en la presente memoria como un circuito configurado (o adaptado) para realizar diversas operaciones predefinidas. Las "operaciones predefinidas" son las operaciones incorporadas en el HDL (u otro lenguaje de definición como Verilog o VHDL).

En una realización ilustrativa, el sistema 2100 de circuitos de control es una FPGA segura.

La figura 21 ilustra una realización de las operaciones predefinidas para el cifrado del sistema 2100 de circuitos de control. Esta realización supone que un mensaje *M* de texto sin formato se procesa secuencialmente en partes apropiadas para el componente analógico 100 particular. Para el ejemplo del componente analógico 100 mostrado en las figuras 1A a 18, la parte apropiada es de dieciséis bits. Para la realización ilustrativa de 256 bits, la parte es de doscientos cincuenta y seis bits. A continuación, la parte del tamaño apropiado se denomina generalmente un fragmento.

Los símbolos usados en la figura 21 se describen ahora.

En la figura 21, el mensaje *M* de texto sin formato tiene una longitud $|M|$ y está dividido en *m fragmentos* M_i donde $i = 1,\ldots,m$. El símbolo M_i representa el fragmento *i-ésimo* del mensaje *M* de texto sin formato.

La figura 21 incluye la idea de un flujo de claves S que también puede denominarse flujo de claves digital *S*. El flujo de claves se genera en m fragmentos Si, donde $i = 1,\ldots,m$. Se genera un S_i para cada M_i.

El texto cifrado *C* se genera en *m* fragmentos C_i donde $i = 1,\ldots, m$ para $Ci = M_i$ XOR S_i.

N es un nonce. *K1* y *K2* son claves de 256 bits. $E1_{K1}(N + i - 1)$ es un cifrado de uno menos que la suma de los nonce *N* e *i* usando *K1*. $E2_{K2}(N + i - 1)$ es un cifrado de uno menos que la suma de los nonce *N e i usando K2.*

El componente analógico, ya sea la versión de 16 bits, la versión de 256 bits u otra realización ilustrativa, se representa como *A*. La entrada del componente analógico es A_i, y la salida del componente analógico es A_o.

Teniendo en cuenta lo anterior, una función E_K viene dada por $E_K(x) = E1_{K1}(A(E1_{K1}(x))) \oplus E2_{K2}(x)$ donde *x* es un conjunto de bits. En la expresión anterior, el término $A(E1_{K1}(x))$ puede interpretarse como el resultado de usar $E1_{K1}(x)$ como la entrada A_i de componente analógico para accionar el componente analógico *A.* Este resultado también se conoce como A_o.

Con esta definición de $E_K(x)$, el flujo de claves *S* puede darse después de modo conciso dado por el $S := \left|\right|_{i=1}^{m} E_K\left(N + i - 1\right)$ donde las dos barras verticales se refieren a una operación de concatenación. Del mismo modo, el texto cifrado *C* puede darse de forma concisa mediante $C = M \oplus S$ para los primeros bits $|M|$ de *M*.

El procesamiento en la figura 21 comienza cuando va a cifrarse algún mensaje *M* de texto sin formato. Se inicializa un contador en s2110. El primer fragmento M_i de bits se obtiene en s2120. Si el fragmento es demasiado corto, se rellena para tener valores suficientes para formar un fragmento. Si se rellena un fragmento, el relleno se descarta más adelante y no se incluye en el texto cifrado *C.*

El procesamiento continúa con s2130, donde la suma de uno menos que la suma de nonce *N* e *i* se cifra con $E1_{K1}$. En la etapa s2140, ese resultado se usa para accionar las líneas 120 de señal de los primeros electrodos del componente analógico 100, lo que provoca que algunos de los primeros electrodos 320 se carguen y, por lo tanto, alteren la orientación de los cristales líquidos en la celda 1600 de cristal líquido. La salida de los sensores 1164 se representa en forma digital y se obtiene como A_o, que también puede escribirse como $A_o = A(E1_{K1}(N+i-1))$. Para decirlo de otro modo, el término $A(E1_{K1}(N+i-1))$ se basa en la representación digital de la salida del componente analógico.

En s2150, ese resultado se cifra nuevamente usando *K1* para dar $E1_{K1}(A(E1_{K1}(N+i-1)))$.

El procesamiento en s2130 hasta s2150 empleó un primer cifrado y una clave *K1.* De hecho, usó el primer cifrado dos veces: una vez con *N+i-1* para generar la entrada del componente analógico, y otra vez en la salida del componente analógico. Este primer cifrado es un cifrado de bloques en una realización ilustrativa. El procesamiento en s2160 usa un segundo cifrado y una clave *K2* diferente de la clave *K1.* El segundo cifrado también es un cifrado de bloques en una realización ilustrativa. En s2160, el segundo cifrado se realiza con *N+i-1* para generar $E2_{K2}(N = I - 1)$.

En s2170, se realiza una operación XOR para obtener S_i.

En s2180, se realiza una operación XOR con M_i y S_i para dar C_i.

En s2190, si quedan por procesar más fragmentos M_i de *M*, entonces el procesamiento continúa con s2195 seguido de s2120. Incrementar el contador en s2195 sirve para avanzar el procesamiento al siguiente fragmento *Mi*. Por otro lado, si no quedan más fragmentos por procesar, el cifrado finaliza, excepto para descartar cualquier relleno que se haya introducido.

La figura 22 muestra las operaciones predefinidas para el sistema 2100 de circuitos de control en caso de descifrado.

La figura 22 es idéntica a la figura 21 con dos excepciones. En s2220 se obtiene un fragmento C_i del texto cifrado C en lugar de un fragmento del mensaje *M de texto sin formato.* En la versión s2280, se realiza una operación XOR con C_i y S_i para obtener M_i.

La similitud entre el proceso de cifrado mostrado en la figura 21 y el proceso de descifrado mostrado en la figura 22 es posible en parte debido al hecho de que, dado que $M \oplus S = C$ se usa en el proceso de cifrado, el uso de $C \oplus S$ en el proceso de descifrado permite reescribir como (M) S sustituyendo por *C*, dando *M.* Por lo tanto, el mismo sistema 2100 de circuitos de control que realiza el cifrado también puede usarse para realizar el descifrado, dependiendo de si el mensaje *M* de texto sin formato se usa como la entrada o si se usa el texto cifrado *C* en su lugar. El control de las operaciones de conversión entre el texto cifrado y el texto sin formato puede, sin pérdida de función, puede materializarse prácticamente del mismo modo en módulos de software o lógica implementados por un microprocesador de uso general.

Pueden proporcionarse aspectos adicionales del sistema 2100 de circuitos de control para mejorar la seguridad del aparato 2000 de seguridad de datos.

Implementación detallada

Ahora se analizará una implementación más detallada de las operaciones predefinidas del sistema 2100 de circuitos de control en el contexto de una realización ilustrativa. En esta realización ilustrativa, las operaciones más detalladas implementan el cifrado autenticado con un componente analógico (AEA, en inglés) como un tipo específico de cifrado autenticado (AE, en inglés).

En una realización ilustrativa, el cifrado de bloques E1 es una red de sustitución-permutación según la figura 23. El cifrado de bloques E1 tiene una longitud de bloque de 256 bits y un tamaño de clave de 256 bits. Acepta como entradas una X de texto sin formato de 256 bits y una clave *K* de 256 bits, y produce el texto cifrado de 256 bits correspondiente $Y = E1_k(X)$.

El cifrado E2 de bloques se usa para establecer un nivel básico de seguridad que depende únicamente de los componentes digitales. El cifrado E2 de bloques está diseñado, en este ejemplo, como una variante de E1 y su estructura global también se muestra en la figura 23. Es una red de sustitución-permutación con una longitud de bloque de 256 bits y un tamaño de clave de 256 bits. Acepta como entradas una X de texto sin formato de 256 bits y una clave maestra *K* de 256 bits, y produce el texto cifrado de 256 bits correspondiente $Y = E2_k(X)$.

En una realización ilustrativa, E2 comparte con E1 la estructura del SPN global y la estructura de la transformación de la ronda y el cronograma clave. Sin embargo, los componentes de la capa de sustitución, la capa de difusión, y la derivación de clave redonda son diferentes de los de E1.

Capa de sustitución: Se usa una caja S de 8 bits no lineal diferente.

Capa de difusión: Se usa una matriz MDS de 32 × 32 diferente.

Adición clave: Se usan diferentes constantes redondas de 256 bits para derivar las subclaves de la clave maestra.

E1 y E2, en una realización ilustrativa, son redes de sustitución-permutación con capas de difusión MDS completas, similares al cifrado de bloques SHARK (véase Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers, Erik De Win: The cipher SHARK. FSE 1996, LNCS 1039, págs. 99-111). A diferencia del AES, aplican una matriz MDS a todo el estado en cada ronda, y no solo a una columna. Si bien es algo más pesado en términos de eficiencia de implementación, esto conduce a una difusión muy rápida (la difusión completa se alcanza después de solo 1 ronda) y a una disminución significativamente más rápida de las propiedades criptoanalíticas a lo largo del número de rondas. La siguiente tabla proporciona una comparación del E1/E2 con el SHARK y el AES.

	E1/E2	SHARK	AES
Longitud de bloque	256 bits	64 bits	128 bits
Tamaños clave	256 bits	128 bits	128/192/256 bits
Rondas	16	6	12/10/2014
Capa caja-S	Caja-S aleatorio de 8 bits	Caja-S de inversión de 8 bits	Caja-S de inversión de 8 bits
Capa lineal	MDS completo (32 × 32)	MDS completo (8 × 8)	Columnas mixtas (4 × 4 MDS)
Difusión total	1 ronda	1 ronda	2 rondas
Cajas S activas	33 por 2 rondas	9 por 2 rondas	25 por 4 rondas

AEA

AEA es un modo de cifrado autenticado (AE), según el concepto inventivo, que usa los cifrados de bloque E1 y E2, así como el componente analógico A, que asigna entradas de 256 bits a salidas de 256 bits. El modo AEA no asume que el componente analógico *A* sea estrictamente biyectivo y puede tolerar algunas imperfecciones en la biyectividad. Sin embargo, el componente *A* es *una* función determinista, lo que significa que entradas iguales producirán salidas iguales.

AE

Uno de los objetivos de los esquemas de cifrado autenticado (AE) es proporcionar simultáneamente confidencialidad y autenticidad/integridad. Esto puede lograrse mediante la combinación de algoritmos de cifrado tal como el cifrado de bloques, con mecanismos de autenticidad e integridad, como los *códigos de autenticación de mensajes (MAC, en inglés)*.

Tras la entrada de un mensaje y una clave, un algoritmo AE genera el texto cifrado correspondiente, así como una etiqueta de autenticación. Durante el descifrado, se verifica esta etiqueta de autenticación. Tras una verificación exitosa, se devuelve el texto sin formato; de lo contrario, se indica el error y no se revela ningún texto sin formato. El concepto clave es que solo los poseedores de la clave pueden producir etiquetas de autenticación válidas, y cualquier modificación en el tránsito del texto cifrado o la etiqueta (o ambos) provocará un error de verificación con alta probabilidad.

Al igual que los modos de operación del cifrado de bloques, muchos esquemas de AE también toman un *nonce* como una entrada (número que se usa una vez, que es público pero no se repite con la misma clave). La entrada nonce tiene que ser idéntica para el cifrado y el descifrado de un mensaje particular.

La operación se ilustra en la figura 24, que muestra el cifrado autenticado no basado en nonce. El remitente transmite el nonce *N,* el texto cifrado *C* y la etiqueta *T*. El nonce *N* solo se usará para un único mensaje con la misma clave.

Interfaz

El modo de operación AEA para el cifrado autenticado toma como entrada

1. una clave secreta K de 512 bits que incluye una clave secreta K1 de 256 bits y una clave K2 secreta de 256 bits, es decir, K = (*K1, K2*);

i) La tecla *K1* puede integrarse estrechamente con el componente analógico *A, p. ej.,* en un chip ASIC;

ii) La clave *K2* puede colocarse fuera del módulo de hardware que contiene el componente analógico *A*, p. ej., en una FPGA o en un software de usuario, para establecer un nivel básico de seguridad para el cifrado autenticado;

2. un nonce *N* de 256 bits (número usado una vez);

3. una entrada *M* de mensaje de longitud $0 \leq |M| < 2^{128}$ bits.

Cuando se usa para el cifrado y la autenticación, genera un texto cifrado de igual longitud que la entrada del mensaje, junto con una etiqueta de autenticación *T* de 256 bits de longitud:

$$AEA\text{ - CIFRAR: } (K, N, M) \rightarrow (C, T).$$

Cuando se usa para el descifrado y la verificación, genera el texto sin formato recuperado junto con un símbolo "S""S" para una verificación exitosa; o no aparece ningún mensaje y una “F” para un error de verificación:

$$AEA\text{ - VERIFICAR: } (K, N, C, T) \rightarrow (M, \{S, F\}).$$

Se supone que la entrada nonce es pública, pero se requiere que sea única en el sentido de que cualquier combinación de (*K, N*) solo debe usarse una vez. Los nonces menores de 256 bits se rellenan con ceros en una cadena de 256 bits. En general, si se requiere el procesamiento de hasta bloques 2^t de mensajes para una única clave, el nonce debería tener una longitud de 2^t bits, debido a la paradoja de la fecha de creación.

A continuación, se definen varios bloques de construcción y finalmente los algoritmos de cifrado y descifrado/verificación AEA.

Modo CTR

El bloque de construcción CTR(N, K, M) toma un nonce N de 256 bits, una clave *K* de 512 bits y una entrada de mensaje *M* (de longitud $0 \leq |M| < 2^{128}$ bits) y produce un texto cifrado *C* de igual longitud a través de:

$$m := \left\lceil \frac{|M|}{256} \right\rceil$$

$$S := E_K(N) || E_K(N + 1) || \cdots || E_K(N + m - 1)$$

$$C := M \oplus S\ [\text{first} \mid M \mid \text{bits}]$$

return C

con la función $E_K(M)$ definida como $E1_{K1}(A(E1_{K1}(M))) \oplus E2_{K2}(M)$. El funcionamiento de la función $E_K(M)$ y el modo de cifrado CTR que usa esta función se ilustran gráficamente en las figuras 26 y 25, respectivamente.

CBC-MAC

El bloque de construcción CBC(K, M) toma una clave K de 512 bits y una entrada de mensaje M (de longitud $0 \leq |M| < 2^{128}$ bits, y un múltiplo de 256 bits) y genera el cifrado del último bloque del mensaje en modo CBC:

$$(M_1, \ldots, M_m). = M$$

$$C_0: = 0^{256}$$

$$C_i: = E_K(M_i \oplus C_{i-1}) \text{ for } i = 1, \ldots, m$$

return C_m

En este caso, $E_K(M)$ se define como anteriormente para el cifrado CTR. Este algoritmo MAC basado en la función E_K se ilustra en la figura 27.

Relleno

El algoritmo de relleno $PAD(M,L_1,L_2)$ toma como entrada un mensaje M de longitud $0 \leq |M| < 2^{128}$ bits, y dos claves de 256 bits L_1 y L_2. Genera una cadena de bits de longitud $t \cdot 256$, $t \geq 1$ del siguiente modo:

if $|M|$ is a multiple of 256:

return $XORPAD(M, L_1)$

else:

return $XORPAD(M \,||\, 10^{255(|M| \bmod 256)}, L_2)$

En este caso, $XORPAD(M, L)$ XOR coloca la más corta de las dos cadenas de bits M y L en el final de la cadena más larga y genera el resultado.

Algoritmo de código de autenticación de mensajes (MAC)

El algoritmo de MAC $MAC(t, K, M)$ toma como entrada un número entero t de 256 bits, una clave K de 512 bits y un mensaje M de longitud $0 \leq |M| < 2^{128}$ bits. Genera una etiqueta de autenticación del siguiente modo:

$$L: = E_K(0^{256})$$

$$L_1: = E1_L(0^{255}||1)$$

$$L_2: = E1_L(1||0^{255})$$

return $CBC(K, PAD([t]_{256}|M, L_1, L_2)]$,

donde $[t]_{256}$ indica la representación binaria de 256 bits del entero t.

CIFRADO AEA: Cifrado y generación de etiquetas

El algoritmo de cifrado autenticado ENCRIPTACIÓN AEA(K, N, M) toma una clave K de 512 bits, un nonce N de 256 bits y un mensaje M de longitud $0 \leq |M| < 2^{128}$ bits. Genera un texto cifrado C y una etiqueta T de 256 bits del siguiente modo:

$$N': = MAC(0, K, N)$$

$$C: = CTR(N', K, M)$$

$$C': = MAC(1, K, C)$$

$$T: = N' \oplus C'$$

return C, T

El uso de diferentes constantes (número entero *t*) para las dos llamadas MAC garantiza una separación de dominio adecuada entre el procesamiento de los bloques nonce y de texto cifrado.

Se debe tener en cuenta que el texto cifrado siempre tiene la misma longitud que el texto sin formato. El funcionamiento global del algoritmo AEA se representa en la figura 28.

Verificación AEA: Descifrado y verificación de etiquetas

El algoritmo de descifrado y verificación *AEA* - VERIFICAR: *(K, N, C, T) → (M, {S, F}) toma como entrada una clave K de 512 bits, un nonce N de 256 bits, un texto cifrado C y una etiqueta T de 256 bits.* Verifica la etiqueta de autenticación y, en caso de éxito, genera el mensaje descifrado y un símbolo "S" para indicar que se ha realizado correctamente (no debe confundirse con el flujo de claves S descrito anteriormente). Tras la verificación del error, genera un mensaje vacío y el símbolo "F":

if $|T| < 256$ then return 0, "F"

$N' := MAC(0, K, N)$

$C' := MAC(1, K. C)$

$T' := N' \oplus C'$

if $T \neq T'$ then return 0, "F"

$M := CTR(N', K, C)$

return M, "S"

Justificación del diseño y análisis de seguridad

El propósito de definir la rutina de cifrado en modo del contador $E_K(M)$ as $E1_{K1}(A(E1_{K1}(M))) \oplus E2_{K2}(M)$ es enmascarar tanto las entradas como las salidas del componente analógico A mediante una llamada de cifrado de bloques. Al cifrar adicionalmente *M* en paralelo a E2 y ordenar con XOR los resultados, una reconstrucción del flujo de contraclave resultante requiere criptoanalizar tanto la parte analógica E1 mixta como la E2, siendo E1 y E2 cifrados de bloques sólidos diseñados de forma conservadora.

La construcción general del modo de operación autenticado de la AEA no es la misma que la del diseño del EAX (véase M. Bellare, P. Rogaway and D. Wagner, "A Conventional Authenticated-Encryption Mode", 2003). EAX usa una llamada de cifrado de bloques normal para su cifrado en modo del contador en lugar del diseño E1/A/E2 de AEA. Además, el diseño MAC de AEA es diferente al de OMAC. La diferencia es que las dos claves L_1 y L_2 no se derivan de L duplicando repetidamente en el campo finito $GF(2^{256})$, sino que se obtienen cifrando diferentes constantes con el *cifrado de bloques E1, usando L como una clave.* La razón de esto es que la duplicación en un campo finito grande requiere recursos de implementación considerables, mientras que las llamadas de cifrado de bloques adicionales pueden usar los cifrados ya implementados.

AEA usa la implementación directa de los cifrados de bloque E1 y E2, no sus inversos. Esto mejora aún más las características de implementación, especialmente para el hardware.

El modo de operación AEA se beneficia de las propiedades de seguridad demostrables de EAX. Como modo de operación de cifrado autenticado, dos nociones de seguridad son interesantes: privacidad y autenticidad. La privacidad se refiere a la confidencialidad de los textos sin formato, mientras que la autenticidad se refiere a la seguridad contra los ataques de falsificación.

Los autores de EAX demuestran que, para estas dos nociones de seguridad, la ventaja de que cualquier adversario no consulte bloques de mensajes de más de σn bits (posiblemente en muchas consultas) se limita del siguiente modo:

$$\mathrm{Adv}_{\mathrm{EAX}}^{\mathrm{Priv}}(\sigma) \leqslant \frac{9\sigma^2}{2^n},$$

y

$$\mathrm{Adv}_{\mathrm{EAX}}^{\mathrm{Aut}}(\sigma) \leqslant \frac{10{,}5\sigma^2}{2^n} + \frac{1}{2^\tau},$$

donde τ indica la longitud de la etiqueta. Ambos límites son esencialmente límites de la fecha de creación, ya que la ventaja se acerca a 1 tan pronto como $\sigma^2 \approx 2^n$. Para AEA, n = τ= 256, por lo tanto el modo puede considerarse seguro si no se cifran más de 2^{128} bloques para la misma clave. El algoritmo MAC de AEA cumple los requisitos de la prueba de seguridad de OMAC, es decir, que L_1 y L_2 son valores aleatorios independientes siempre que L sea aleatorio.

Aun otra diferencia más entre AEA y EAX se refiere al uso del componente analógico A, que no es necesariamente una biyección. Sin embargo, el análisis de seguridad de EAX en realidad abstrae el cifrado de bloques de concreto y asume funciones aleatorias de n bits a n bits. Los límites de seguridad anteriormente mencionados se derivan usando el supuesto de función aleatoria, lo que significa que se aplican igualmente a AEA si la no biyectividad de A es aproximadamente igual a la probabilidad de colisión de una función aleatoria de 256 a 256 bits, es decir, $1/2^{216}$, y el cifrado de bloques E1 es una permutación pseudoaleatoria segura; o el cifrado E2 de bloques es una permutación pseudoaleatoria segura.

Dado que tanto E1 como E2 están diseñados para ser permutaciones pseudoaleatorias seguras, los límites de seguridad de EAX también se aplican a AEA.

Por último, el análisis de seguridad demostrable de EAX, aplicable a AEA, asume adversarios que no respetan los nonces, por lo que no se ofrecen garantías cuando se repiten los nonces. Por lo tanto, en AEA se usan nonces únicos.

Análisis del compromiso parcial

El análisis de seguridad anterior se aplica al modelo estándar en donde se supone que las claves criptográficas no están comprometidas, y el objetivo del adversario es descifrar el nuevo texto cifrado o falsificar correctamente nuevos mensajes con etiquetas de autenticación válidas. Esto último puede estar en una de dos configuraciones:

Falsificaciones existenciales: Deducción de un nuevo par de mensajes/etiquetas válido sin control sobre el contenido del mensaje.

Falsificaciones universales: Deducción de nuevos pares arbitrarios de mensajes/etiquetas válidos con control total sobre el contenido del mensaje.

Sin claves comprometidas, todo esto es imposible hasta los límites de seguridad comprobados descritos anteriormente.

Ahora se discute el impacto de tener uno o dos de los componentes del cifrado E_K comprometidos. Recuerde que se define como

$$E_K(M) = \mathrm{E1}_{K1}\,(A(\mathrm{E1}_{K1}(M)) \oplus \mathrm{E2}_{K2}(M).$$

En el primer escenario (S1), solo la parte digital $\mathrm{E2}_{K2}$ está comprometida en el sentido de que el adversario puede calcular consultas arbitrarias, es decir, ha logrado extraer o simular su funcionalidad, con o sin conocer la clave *K2*. En el segundo escenario (S2), el adversario ha reconstruido toda la funcionalidad implementada *digitalmente*, es decir, pueden calcularse consultas arbitrarias a $E1_{K1}$ y a $\mathrm{E2}_{K2}$. Esto puede implicar la recuperación de *K1 y K2* o no. Se debe tener en cuenta que este segundo escenario equivale a un compromiso de toda la clave maestra *K =(K1, K2)*.

Seguridad contra el adversario S1

En este escenario, el adversario puede calcular $\mathrm{E2}_{K2}(x)$ para cualquier entrada x. Para los objetivos de seguridad, esto tiene las siguientes implicaciones:

Confidencialidad: Para descifrar un bloque de texto cifrado C_i, el adversario tiene que calcular el flujo de claves del contador $S_i = E_K(N + i - 1)$, lo que requiere conocimientos de $\mathrm{E1}_{K1}(A(\mathrm{E1}_{K1}(N + i - 1)))$ y $\mathrm{E2}_{K2}\,(N + i - 1)$. Como $\mathrm{E1}_{K1}$ y *A* no están comprometidos, no tiene información sobre S_i y, por lo tanto, sobre M_i en texto sin formato.

Falsificación: Como se describió anteriormente, el adversario no puede calcular el flujo de claves del contador si solo conoce el $\mathrm{E2}_{K2}$. El adversario no puede producir textos cifrados correctos que correspondan a los textos sin formato de su elección, lo que descarta las falsificaciones universales. Para las falsificaciones existenciales, el adversario podría intentar calcular una etiqueta correcta para el texto cifrado aleatorio (o el texto cifrado tomado de otras consultas con la misma clave). Sin embargo, esto requiere la capacidad de calcular $E1_{K1}(A(\mathrm{E1}_{K1}(x)))$ para producir cifrados CBC-MAC correctos, que él no tiene.

En resumen, el compromiso de $\mathrm{E2}_{K2}(x)$ no tiene un impacto directo en la seguridad de AEA. Sin embargo, los límites de seguridad demostrables ahora dependen de que $\mathrm{E1}_{K1}(A(\mathrm{E1}_{K1}(\cdot)))$ se comporte como una función aleatoria.

Seguridad contra Adversario S2

En este escenario, el adversario puede calcular $E1_{K1}(x)$ y $E2_{K2}(x)$ para cualquier entrada x. Para los objetivos de seguridad, esto tiene las siguientes implicaciones:

Confidencialidad: Para descifrar un bloque de texto cifrado C_i, el adversario tiene que calcular el flujo de claves del contador $S_i = E_K(N + i - 1)$, lo que requiere conocimientos de $E1_{K1}(A(E1_{K1}(N + i - 1)))$ y $E2_{K2}(N + i - 1)$. Con $E1_{K1}(x)$ y $E2_{K2}(x)$ comprometidos, la seguridad ahora depende completamente del componente *A* que no esté comprometido. Si su probabilidad de colisión es superior a la aleatoria, el límite de confidencialidad correspondiente se reduce a

$$\mathrm{Adv}_{\mathrm{EAX}}^{\mathrm{Priv}}(\sigma) \leqslant \frac{9\sigma^2}{2^{\tau}},$$

para una probabilidad de colisión *A* igual a $1/2^{\tau}$ con $\tau < 256$.

Falsificación: Al igual que en el escenario (S1), la seguridad frente a las falsificaciones existenciales y universales ahora depende por completo del único componente *A* no comprometido. Si su probabilidad de colisión es superior a la aleatoria, el límite de autenticidad correspondiente se reduce a

$$\mathrm{Adv}_{\mathrm{EAX}}^{\mathrm{Aut}}(\sigma) \leqslant \frac{10{,}5\sigma^2}{2^{\tau}} + \frac{1}{2^{256}},$$

para una probabilidad de colisión *A* igual a $1/2^{\tau}$ con $\tau < 256$.

En resumen, el compromiso de $E1_{K1}(x)$ y $E2_{K2}(x)$ no tiene un impacto inmediato en la seguridad de AEA. Sin embargo, su seguridad ahora depende tanto de la incapacidad de clonar la funcionalidad del componente analógico como de su probabilidad de colisión.

Seguridad poscuántica

Al usar ordenadores cuánticos, específicamente el algoritmo de Grover, la raíz cuadrada del espacio de búsqueda puede acelerar el exhaustivo problema de búsqueda de claves para algoritmos de cifrado simétrico como E1 y E2: Una clave de *k* bits puede forzarse brutalmente en el tiempo $O(2\ k/2)$ en lugar de $O(2^k)$ mediante el algoritmo de Grover. Dado que E1 y E2 se proponen con una clave de 256 bits, siguen ofreciendo un nivel de seguridad poscuántico de 128 bits. Una segunda consideración es el tamaño del circuito cuántico (el número de qubits) necesario para implementar realmente el algoritmo de Grover para la búsqueda exhaustiva de claves para un cifrado de bloques concreto. Un estudio reciente (M. Grassl y col.: Applying Grover's Algorithm to AES: Quantum Resource Estimates, PQCrypto 2016) estima que se necesita un circuito cuántico con un total de 6681 qubits para atacar el AES-256. La complejidad temporal se estima en $1{,}44 \times 2^{151}$ operaciones. Dado que E1 y E2 están diseñados con un tamaño de estado mayor, deberían requerir al menos los recursos antes mencionados para un ataque cuántico exitoso.

Una segunda preocupación es la seguridad poscuántica del modo de operación (AEA). Como modo compuesto, su seguridad se basa en la seguridad de los modos de operación CBC y CTR subyacentes. Es bien sabido que tanto el CBC como el CTR proporcionan seguridad IND-CPA (falta de capacidad de ser indistinguible en los ataques de texto sin formato seleccionados) contra los atacantes cuánticos bajo el supuesto estándar de PRF siempre que el algoritmo de cifrado se implemente de forma clásica. Esto significa que un atacante cuántico solo puede usar algoritmos cuánticos para procesar consultas de cifrado regulares y, en particular, no realizar consultas de cifrado cuántico. Esta situación cambia cuando el algoritmo de cifrado también se implementa en una computadora cuántica, y se permite al adversario realizar consultas cuánticas en los mensajes superpuestos. Un estudio reciente (M. Anand y col.: Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation, PQCrypto 2016) muestra que, en este caso, la suposición estándar de PRF no cuántica sobre los cifrados de bloques subyacentes solo es suficiente para obtener el Ind- qCPA para el CTR, pero no para el CBC. Para tener la seguridad Ind-qCPA para el CBC, el cifrado de bloques subyacente debe ser un qPRF (PRF cuántico seguro).

Variante basada en AES

En realizaciones alternativas, los cifrados de bloques dedicados E2 y/o E1, tal como se usan en AEA, pueden reemplazarse por una construcción de cifrado de bloques basada en AES. Dado que el AES es un cifrado de bloques de 128 bits, se convierte en un cifrado de bloques de 256 bits mediante una red Feistel equilibrada que usa AES-256 (con claves de 256 bits) como la función F. El cifrado de una entrada *X* de 256 bits a un texto cifrado *Y* bajo una clave *K* de 256 bits se proporciona entonces del siguiente modo:

$$L_0 || R_0 := X$$

$$L_{i+1} := R_i$$

$$R_{i+1} := L_i \oplus F(R_i, K_i) \text{ for } i = 0, \ldots. 9;$$

$$Y := L_{10} || R_{10}$$

La función F se define como

$$F(R_i, K_i) = \text{AES-256}_{Ki}(R_i)$$

y las teclas redondas

$$K_i = K \oplus (i + 1).$$

Siempre que el AES-256 sea un cifrado de bloques seguro, entonces el resultado de Dai y Steinberger (Yuanxi Dai, John Steinberger: Indifferentiability of 8-round Feistel networks, CRYPTO 2016) implica la indivisibilidad de una permutación aleatoria después de 8 rondas y se añaden 2 rondas para obtener un margen de seguridad adicional.

Se debe tener en cuenta que la indivisibilidad es una noción de seguridad extremadamente sólida: por ejemplo, la seguridad frente a todos los ataques de texto sin formato elegidos de forma adaptativa hasta el límite de la fecha de creación (2^{128}) ya se logra después de solo 4 rondas (M. Luby, C. Rackoff, How to construct pseudorandom permutations from pseudo-random functions, SIAM Journal on Computing, vol. 17, n. 2, pp. 373-386, April 1988.)

Ejemplo de interfaz de programación de aplicaciones

Cifrado:

void aea_encrypt(const uint8_t* msg, int len, uint8_t* c, uint8_t tag[32], uint8_t nonce[32], uint8_t key[64]);

Implementa el cifrado autenticado según el algoritmo AEA. Las entradas son las siguientes:

mensaje: Entrada de mensaje, una cadena de bites de longitud "longitud" bites.

longitud: La longitud del "mensaje" en bites puede estar entre 0 y MAXINT.

nonce: nonce de 256 bits (32 bites). Este número debe ser único durante la vida útil de una clave. No es necesario que sea secreto y puede repetirse para diferentes claves. Los nonces menores de 256 bits se rellenan con ceros.

clave: Clave maestra de 512 bits, que comprende K1 y K2 para los cifrados de bloques E1 y E2.

Esta función genera:

c: el texto cifrado. Tiene la misma longitud que la entrada "mensaje".

etiqueta: la etiqueta de autenticación correspondiente a mensaje, key y nonce.

Descifrado y verificación:

bool aea_decrypt(const uint8_t* c, int len, uint8_t* msg, uint8_t tag[32], uint8_t nonce[32], uint8_t key[64]);

Implementa el descifrado y la verificación de etiquetas según el algoritmo AEA. Las entradas son las siguientes:

c: Entrada de texto cifrado, una cadena de bites de longitud "longitud" bites.

longitud: La longitud de "c" puede estar entre 0 y MAXINT.

etiqueta: Etiqueta de autenticación correspondiente a c.

nonce: nonce de 256 bits que se usó para producir el texto cifrado.

clave: Clave maestra de 512 bits, que comprende K1 y K2 para los cifrados de bloques E1 y E2.

Esta función genera:

mensaje: el texto sin formato, tras el éxito de la verificación. Tiene la misma longitud que la entrada "mensaje". Si la verificación de etiquetas falla, esta salida está vacía.

Genera un valor booleano que indica que la verificación se ha realizado correctamente.

A quienes estén familiarizados con esta tecnología se les ocurrirán otras características y funciones, y tales variaciones son de esperar considerando los ejemplos completos y detallados proporcionados anteriormente.

REIVINDICACIONES

1. Un aparato, que comprende:

un componente analógico (100) que tiene:
primeros electrodos (320) conectados eléctricamente con las respectivas líneas (120) de señal de los primeros electrodos, configurándose dichas líneas (120) de señal de los primeros electrodos de tal modo que pueda proporcionarse una entrada de componente analógico A_i al componente analógico (100) a través de dichas líneas (120) de señal de los primeros electrodos, siendo dicha entrada de componente analógico A_i *una* secuencia de valores binarios, o bits;
una celda (1600) de cristal líquido sobre los primeros electrodos (320);
uno o más segundos electrodos (1420) sobre la celda (1600) de cristal líquido y opuestos a los primeros electrodos (320);
una guía (561) de ondas de entrada configurada para introducir una señal óptica constante como una entrada óptica y comunicar la entrada óptica a la celda (1600) de cristal líquido; y
un sensor (1164) configurado para proporcionar una salida del sensor basada en la detección de una salida óptica de la celda (1600) de cristal líquido.

2. El aparato según la reivindicación 1, que comprende además una guía (564) de ondas de salida que comunica la salida óptica de la celda (1600) de cristal líquido al sensor (1164).

3. El aparato según la reivindicación 1, que comprende además:

los primeros electrodos (320) que están dispuestos en filas y columnas;
un ancho y una profundidad de los primeros electrodos que son uniformes entre las columnas; y
una longitud respectiva de los primeros electrodos (320), en las filas que están más alejadas de la guía (561) de ondas de entrada, que es más larga que la longitud respectiva de los primeros electrodos (320) en las filas más cercanas a la guía (561) de ondas de entrada.

4. El aparato según la reivindicación 1, que comprende además una capa (910) de poliimida en contacto con la celda (1600) de cristal líquido y que tiene una alineación molecular irregular.

5. El aparato según la reivindicación 1, que comprende además:

sistema (2100) de circuitos de control adaptados para realizar operaciones predeterminadas, incluida la obtención de datos digitales M con una longitud $|M|$, la determinación del flujo de claves digitales $S = (E1_{K1}(A(\mathrm{E1}_{K1}(N))) \oplus E2_{K2}(N))$, y el cálculo del texto cifrado $C = M \oplus S$ para un primer $|M|$ bits of M;
donde

N es un nonce,
$K1$ y $K2$ son claves,
$E1_{K1}(N)$ es un cifrado de N que usa $K1$,
$\mathrm{E2}_{K2}(N)$ es un cifrado de N que usa $K2$,
A es el componente analógico, y
$E1_{K1}(A(E1_{K1}(N)))$ es un cifrado de $A(E1_{K1}(N))$ que usa $K1$; y
$(A(E1_{K1}(N)))$ se basa en una representación digital de la salida del sensor cuando se usa $E1_{K1}(N)$ para accionar los primeros electrodos (320) del componente analógico (100).

6. El aparato según la reivindicación 3, en donde la longitud de los primeros electrodos (320) se duplica sustancialmente con cada una de las filas sucesivas.

7. El aparato según la reivindicación 1, en donde todos los primeros electrodos (320) están dispuestos por debajo de solo una mitad del ancho de la celda (1600) de cristal líquido.

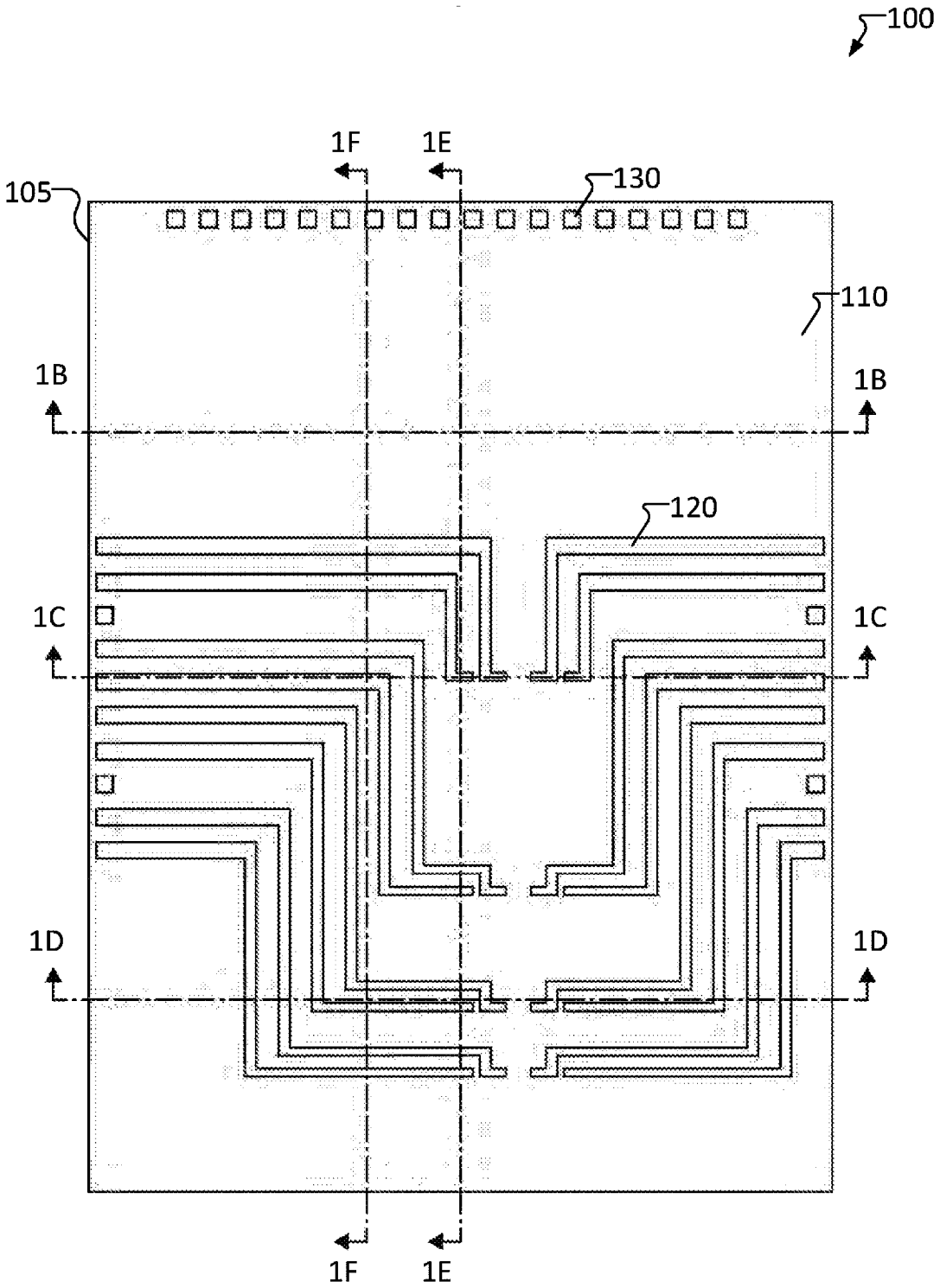

Figura 1A

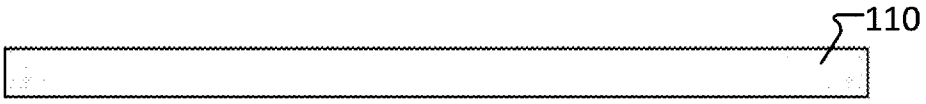

Figura 1B

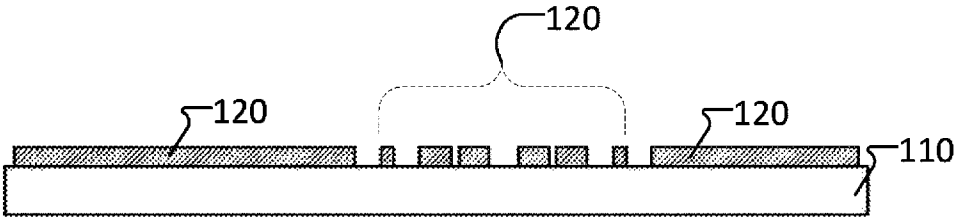

Figura 1C

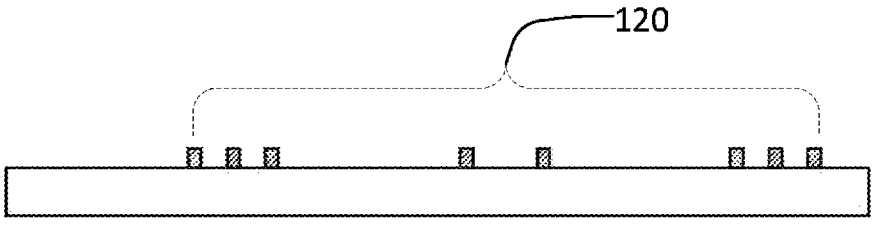

Figura 1D

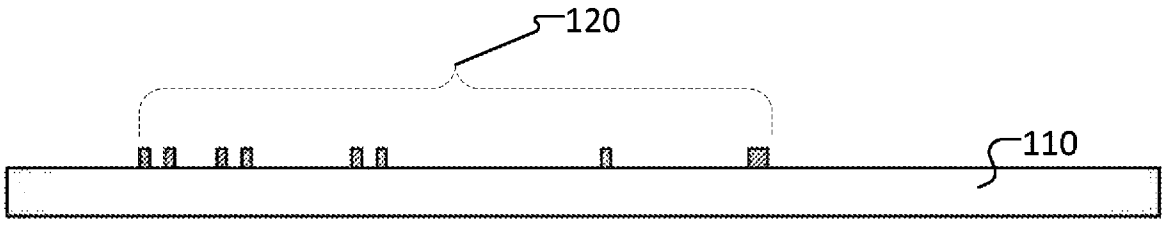

Figura 1E

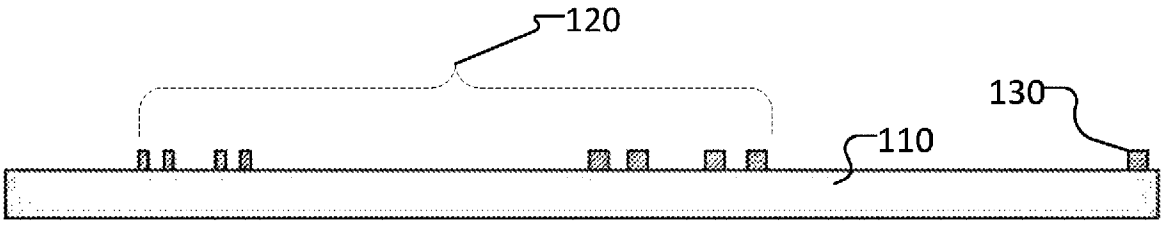

Figura 1F

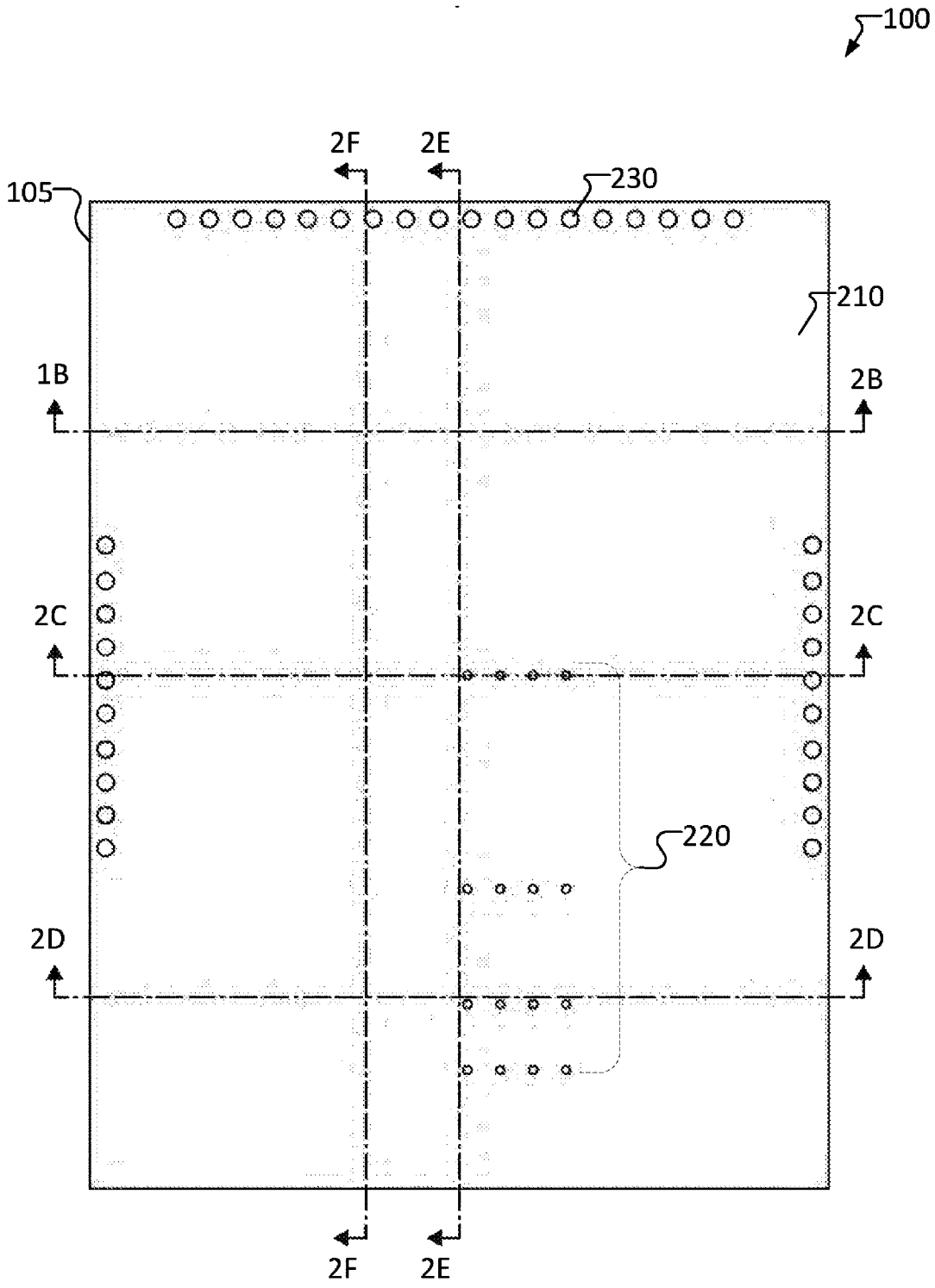

Figura 2A

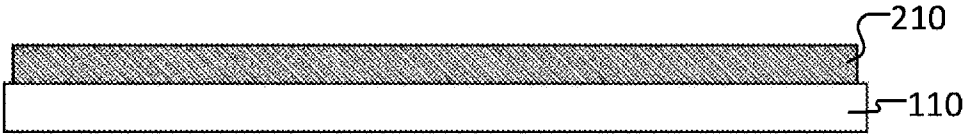

Figura 2B

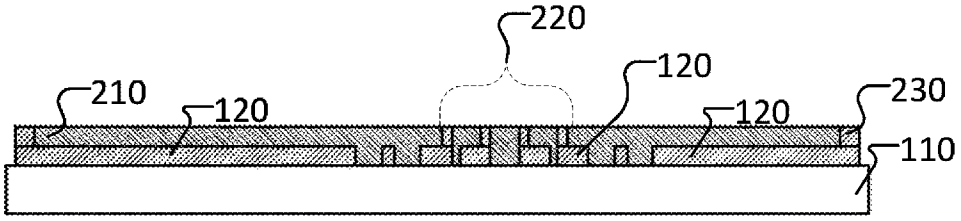

Figura 2C

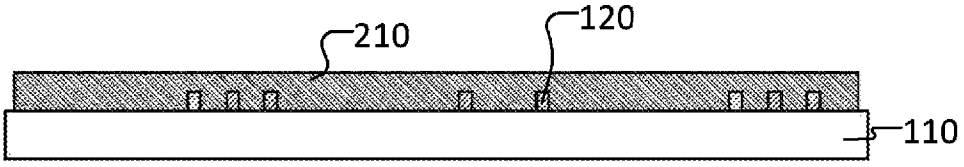

Figura 2D

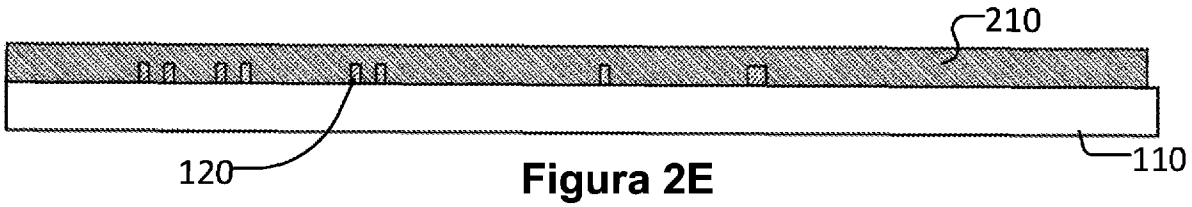

Figura 2E

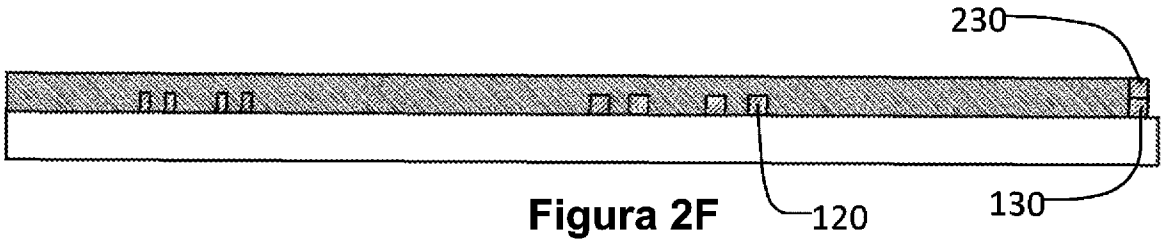

Figura 2F

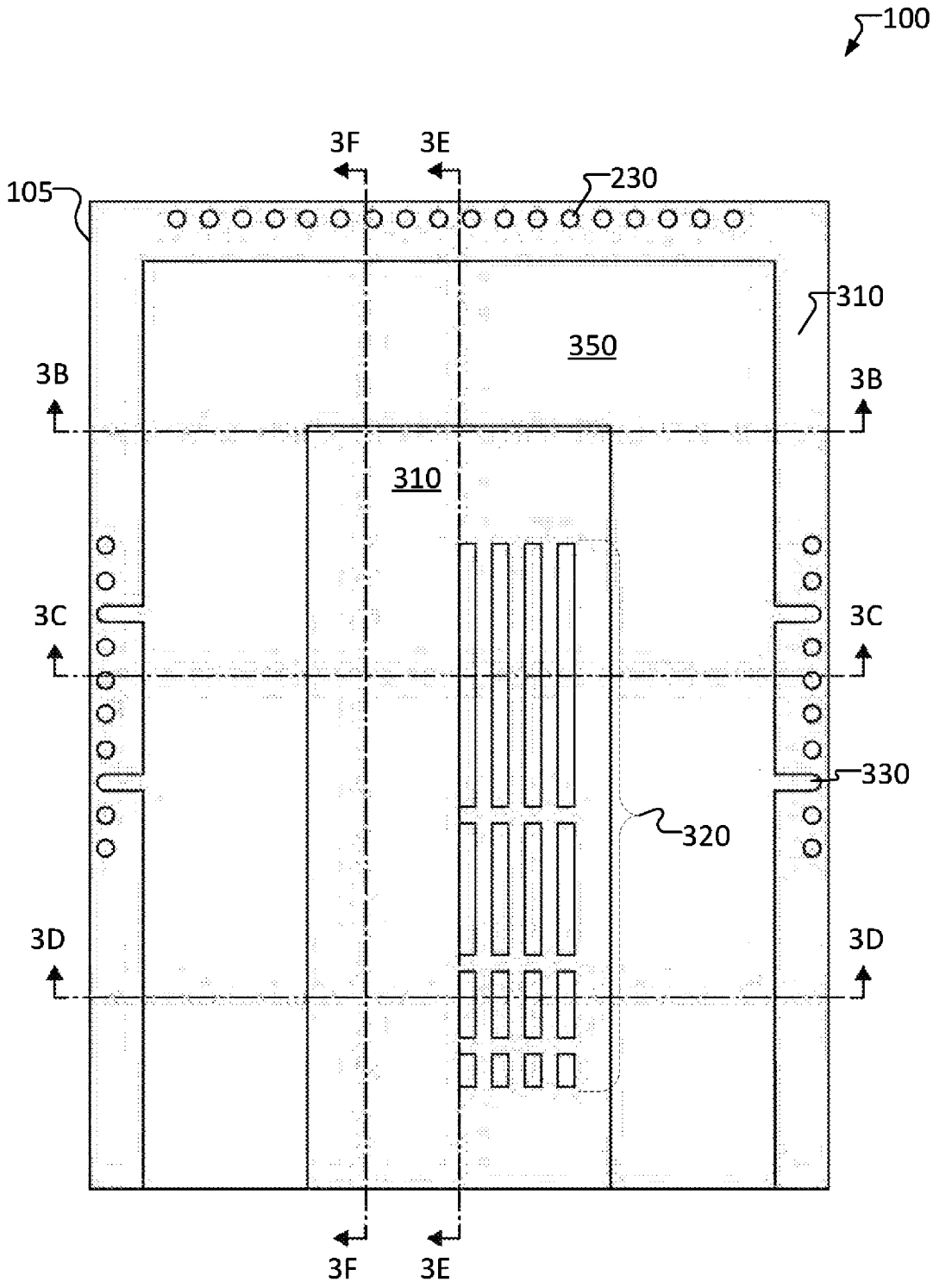

Figura 3A

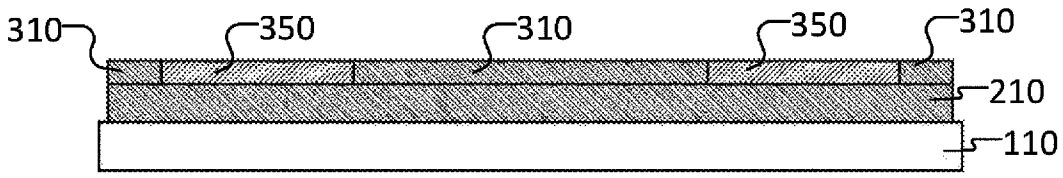

Figura 3B

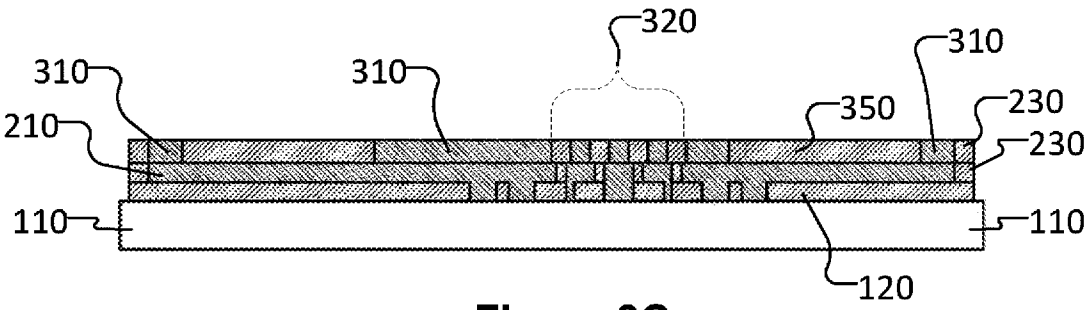

Figura 3C

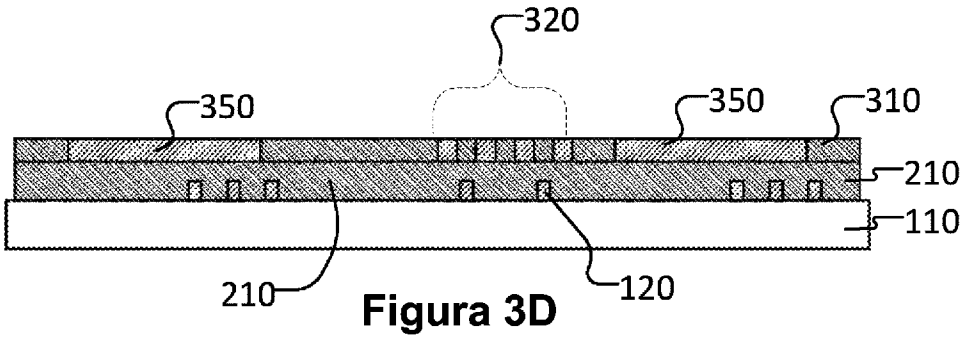

Figura 3D

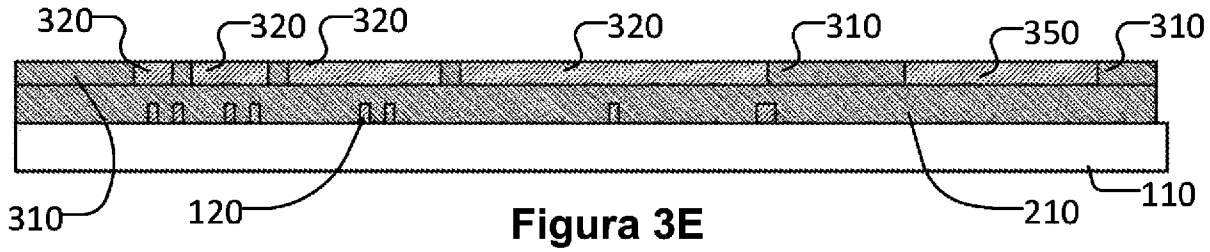

Figura 3E

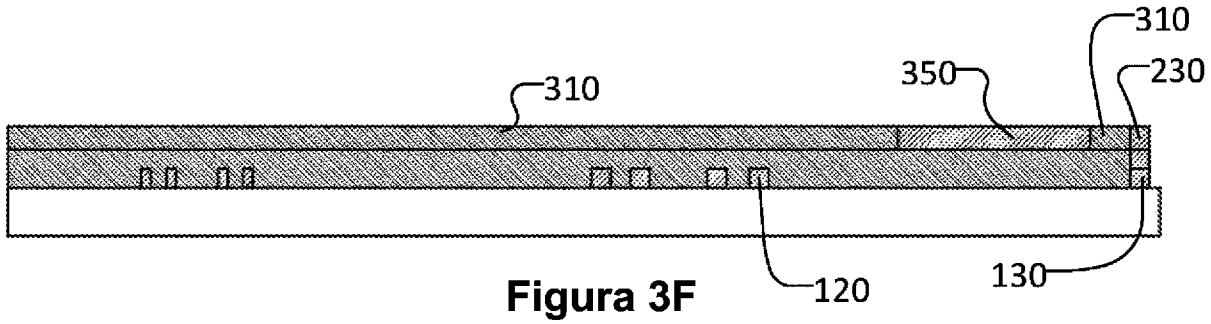

Figura 3F

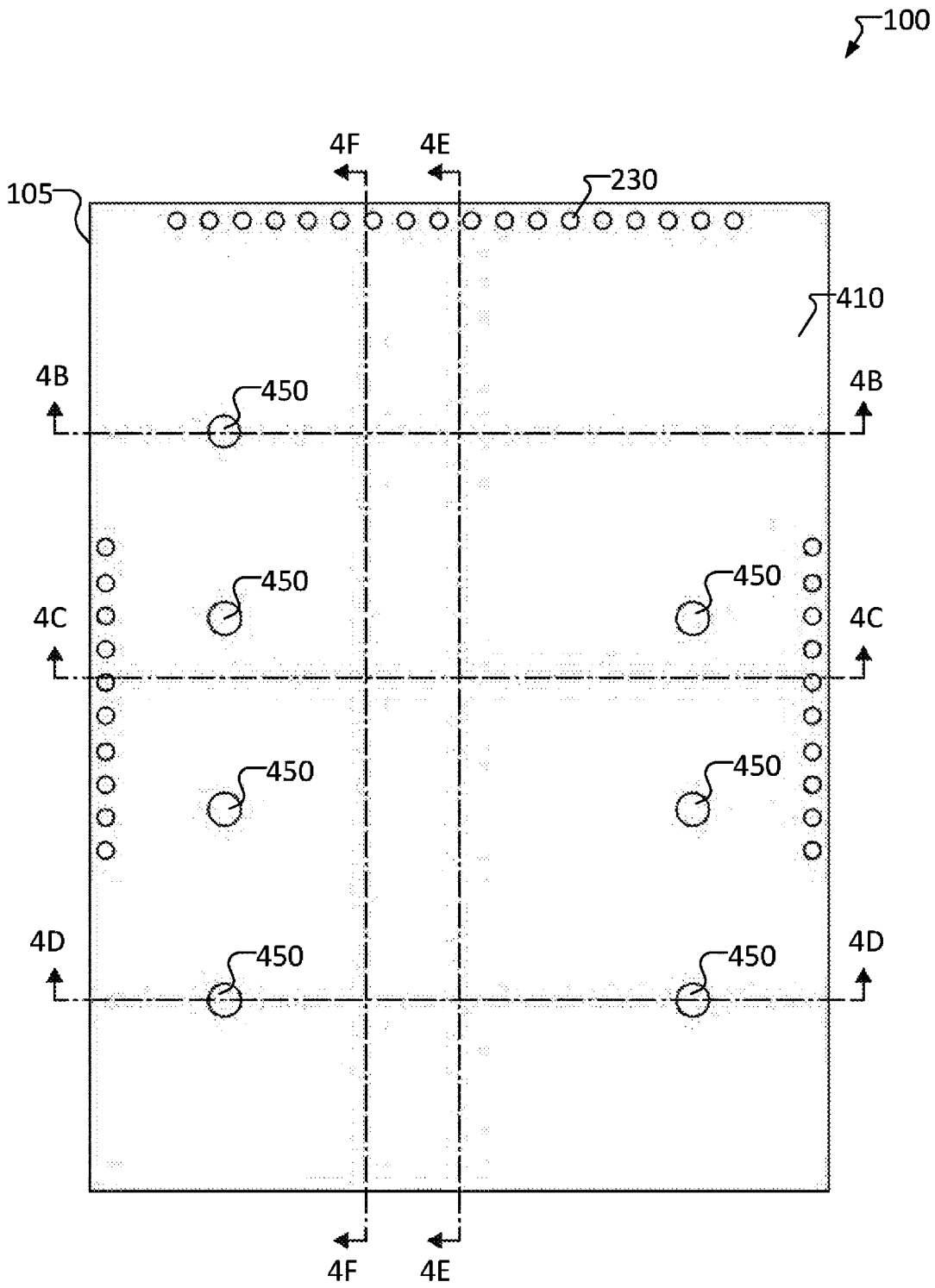
100
4F
4E
105
230
410
4B
450
4B
450
450
4C
4C
450
450
4D
450
450
4D
4F
4E

Figura 4A

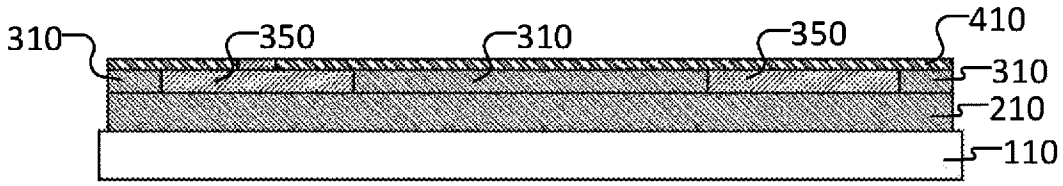

Figura 4B

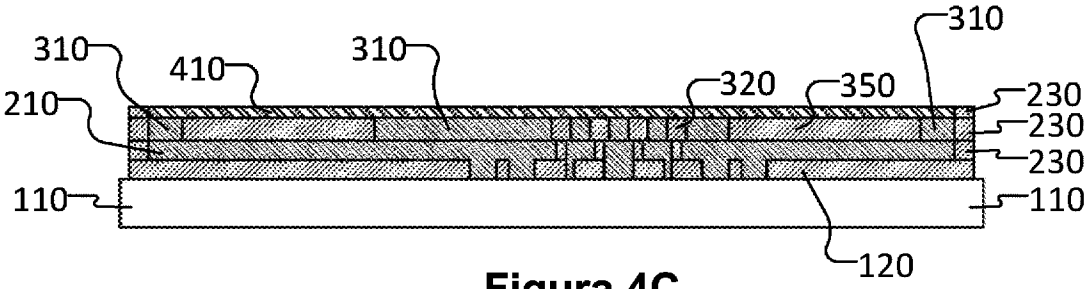

Figura 4C

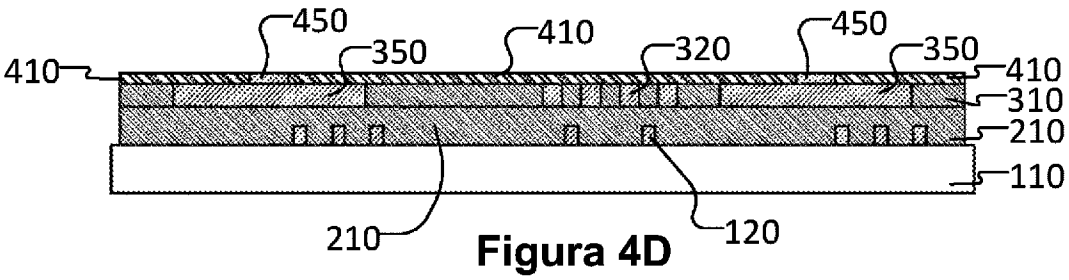

Figura 4D

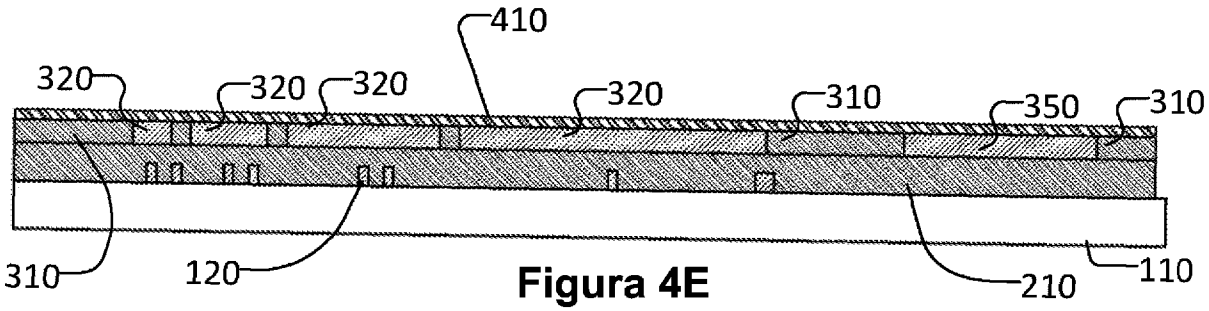

Figura 4E

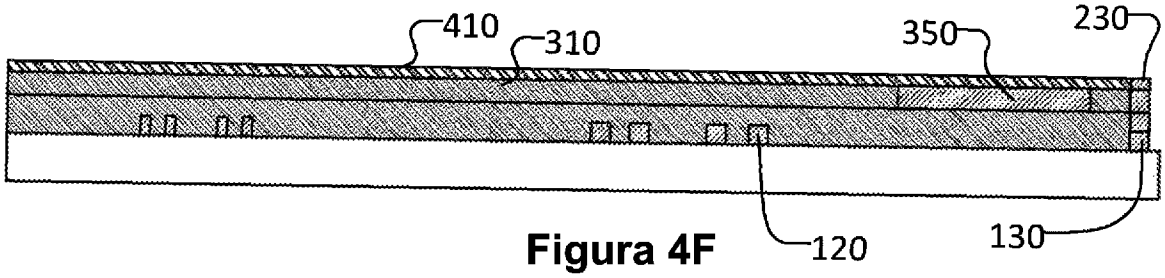

Figura 4F

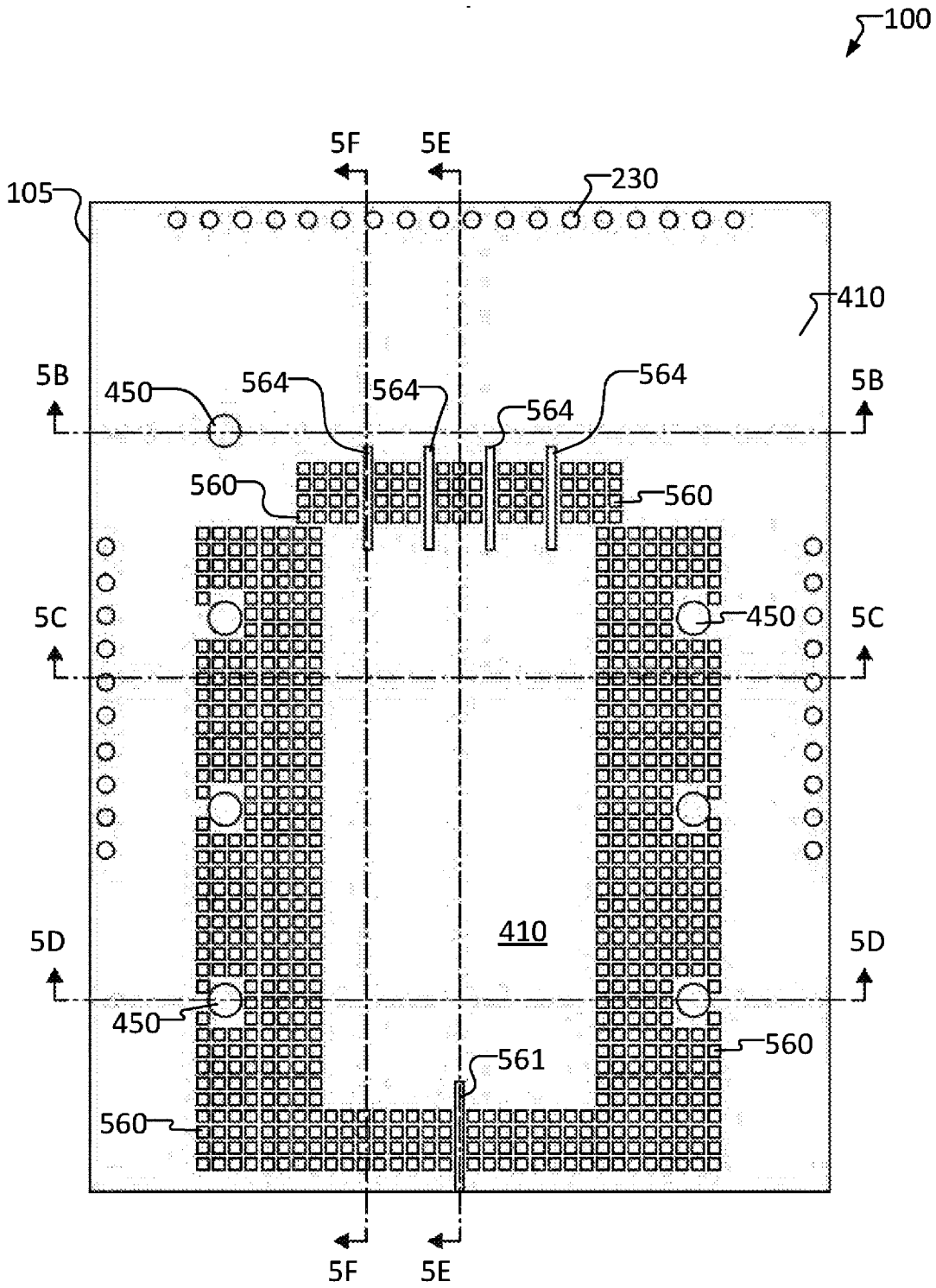
100
5F
5E
105
230
410
5B
450
564
564
564
564
5B
560
560
5C
450
5C
410
5D
5D
450
561
560
560
5F
5E

Figura 5A

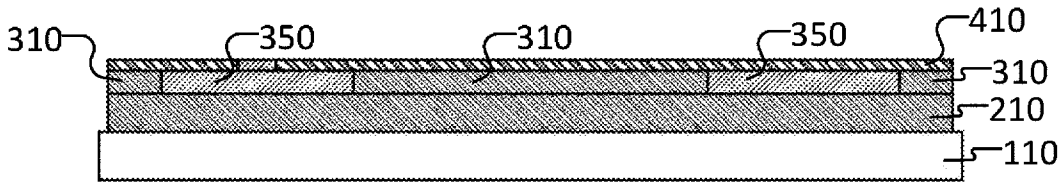

Figura 5B

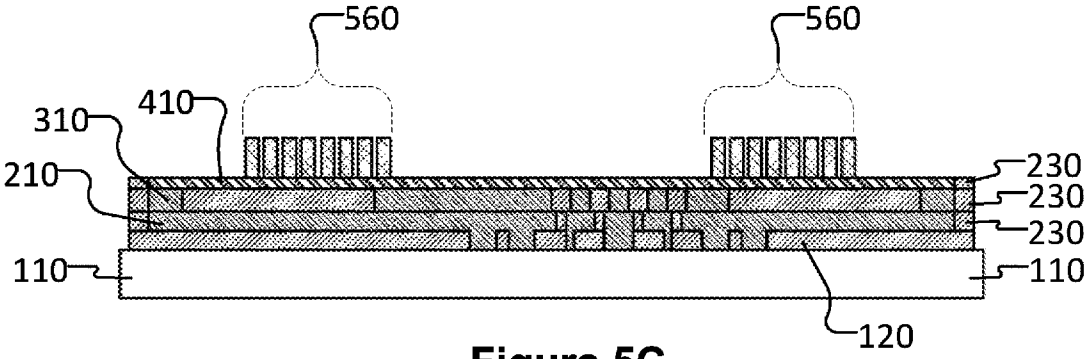

Figura 5C

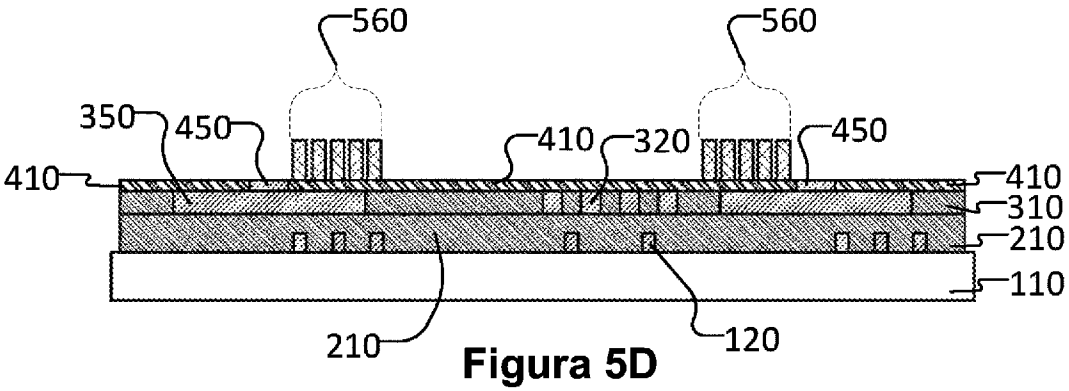

Figura 5D

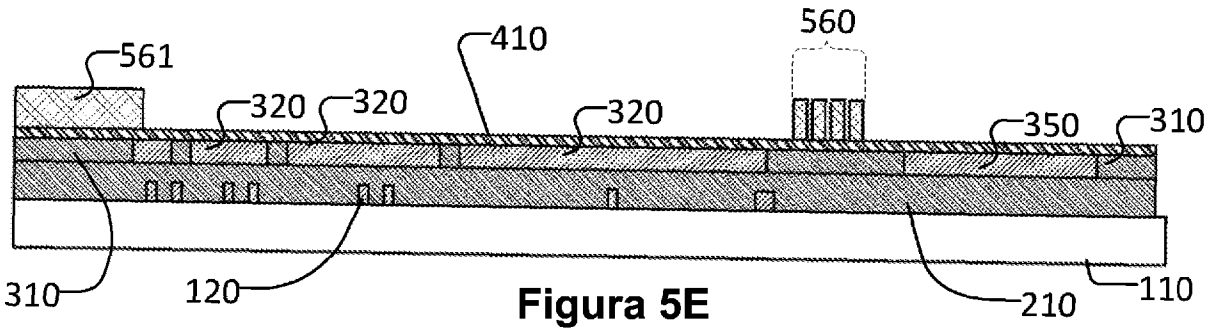

Figura 5E

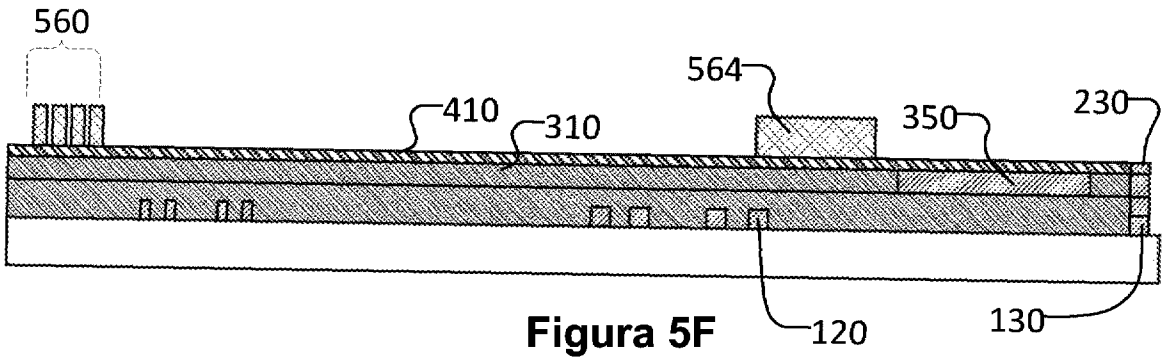

Figura 5F

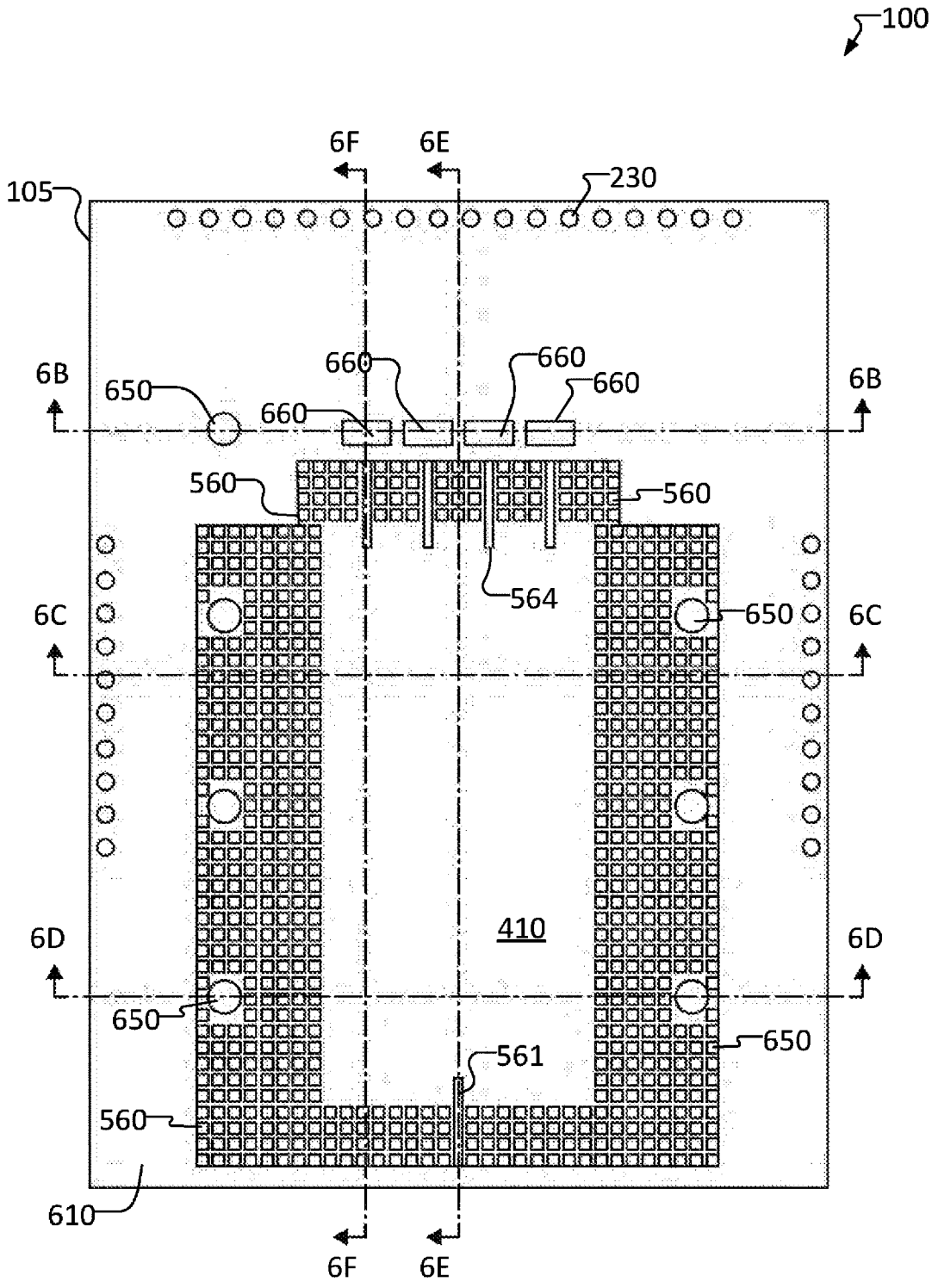
100
6F
6E
105
230
6B
650
660
660
660
660
6B
560
560
564
6C
650
6C
410
6D
6D
650
650
561
560
610
6F
6E

Figura 6A

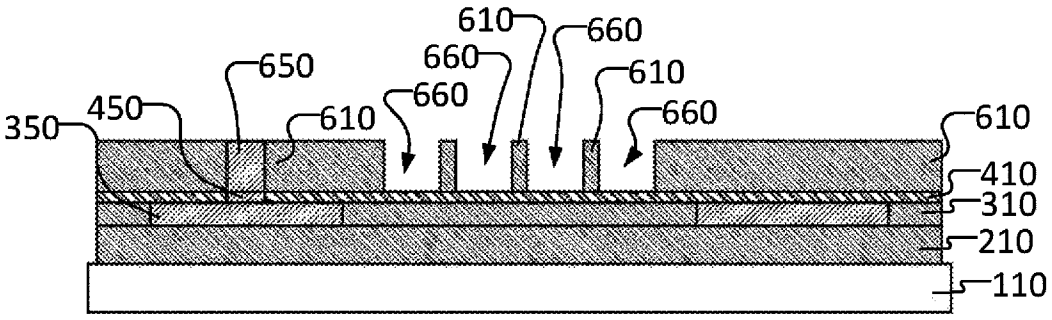

Figura 6B

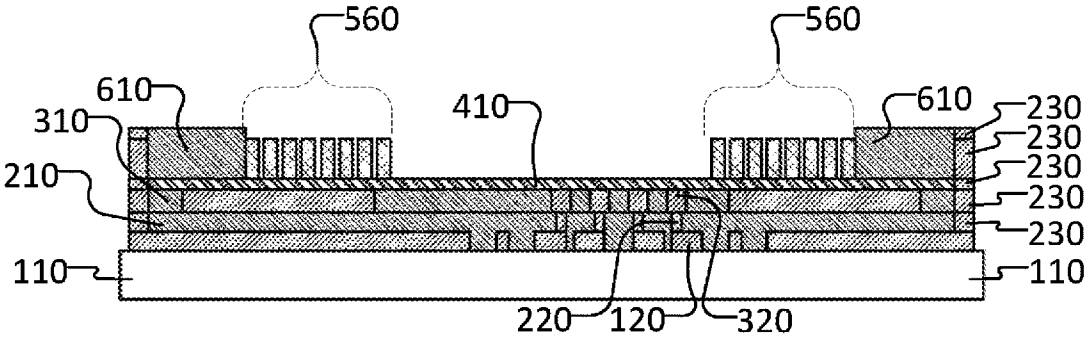

Figura 6C

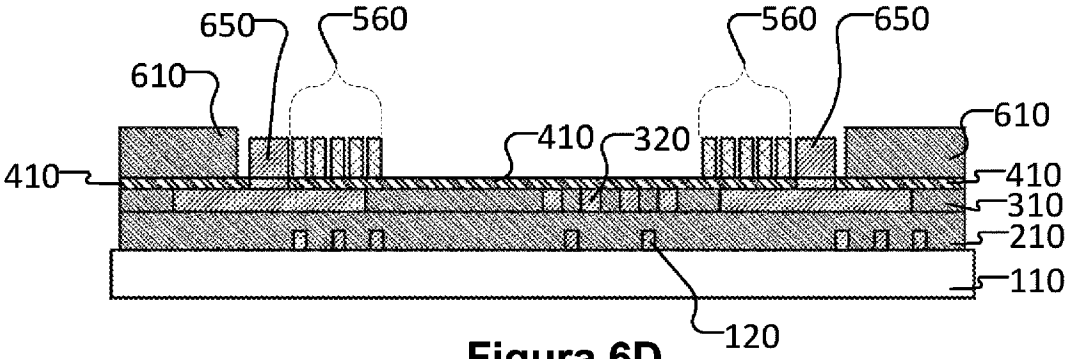

Figura 6D

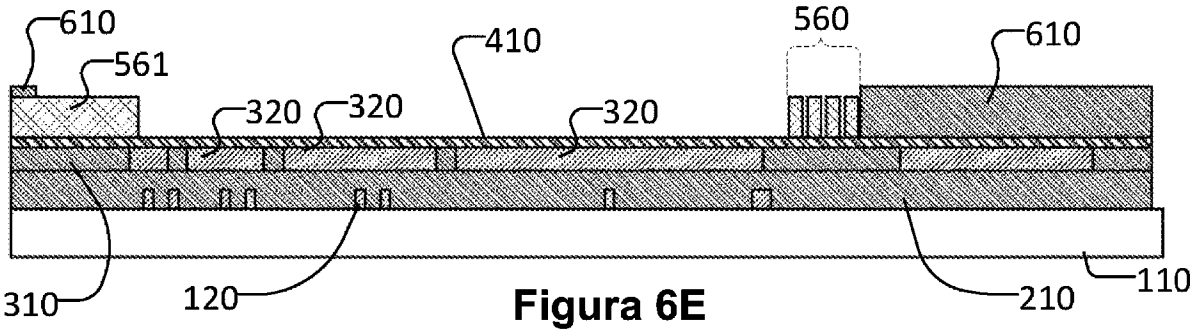

Figura 6E

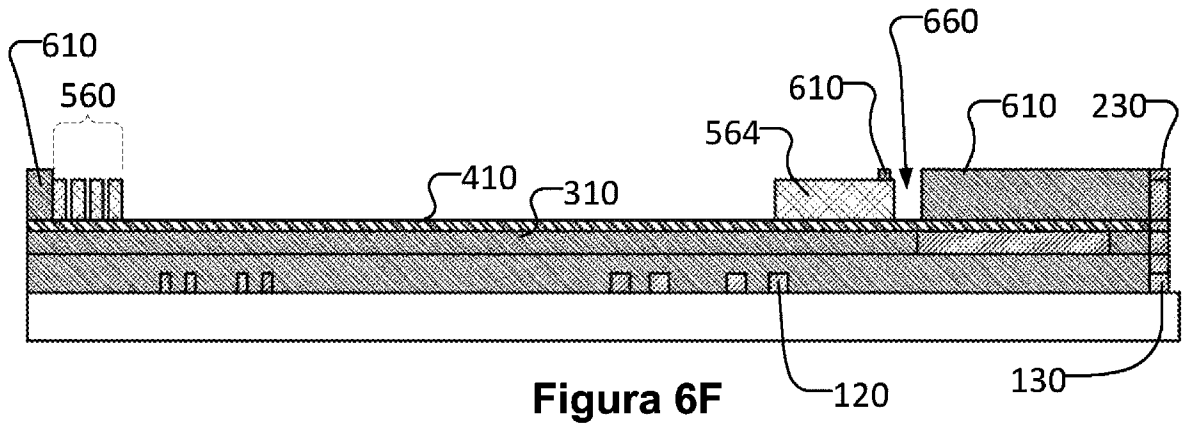

Figura 6F

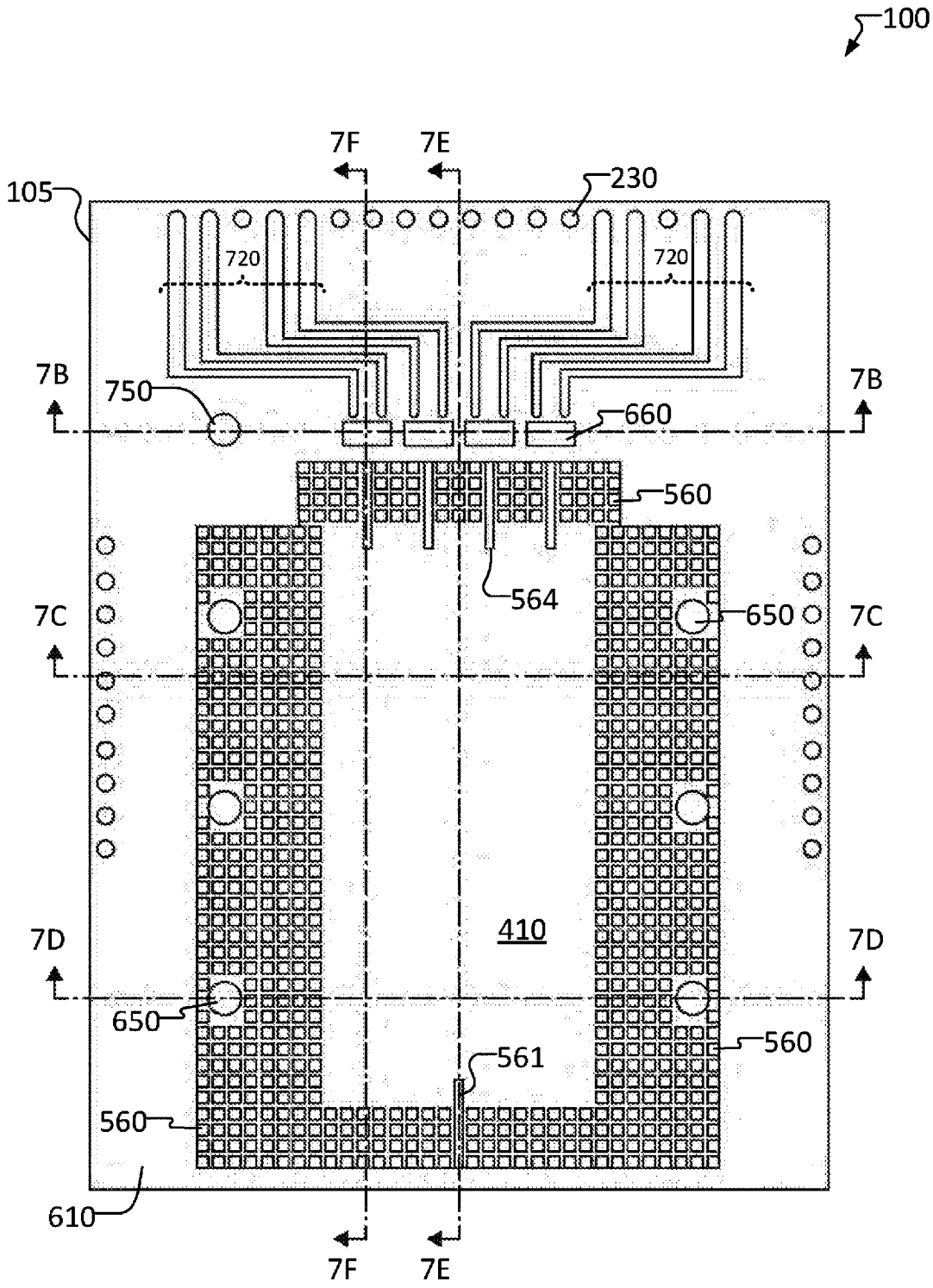
100
7F
7E
105
230
720
720
7B
750
660
7B
560
564
7C
650
7C
410
7D
650
7D
561
560
560
610
7F
7E

Figura 7A

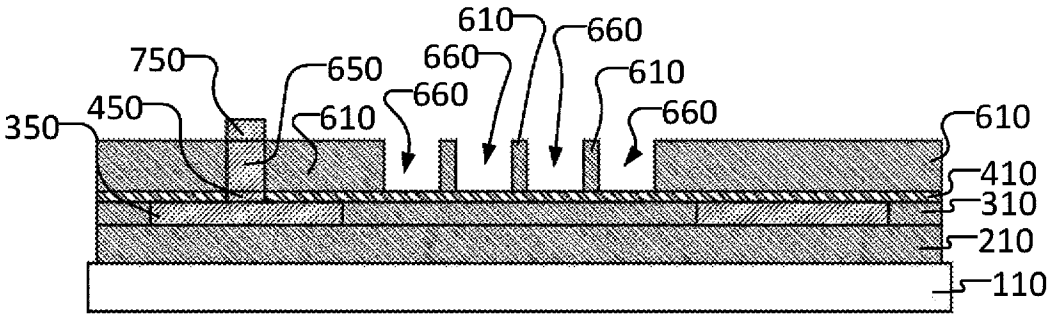

Figura 7B

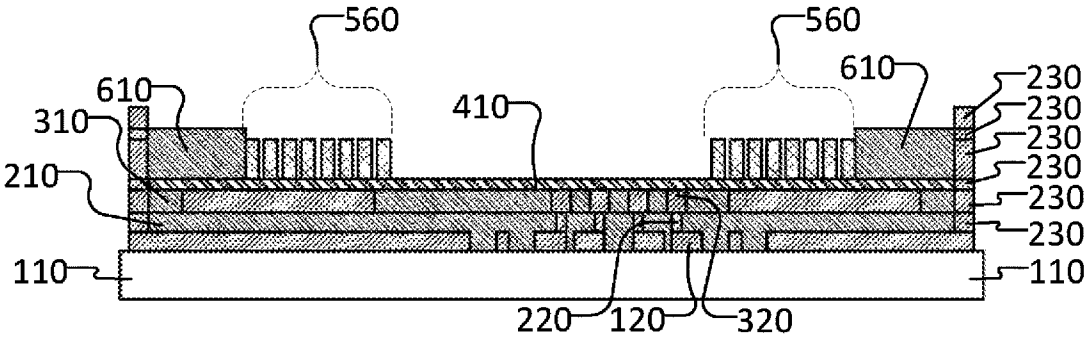

Figura 7C

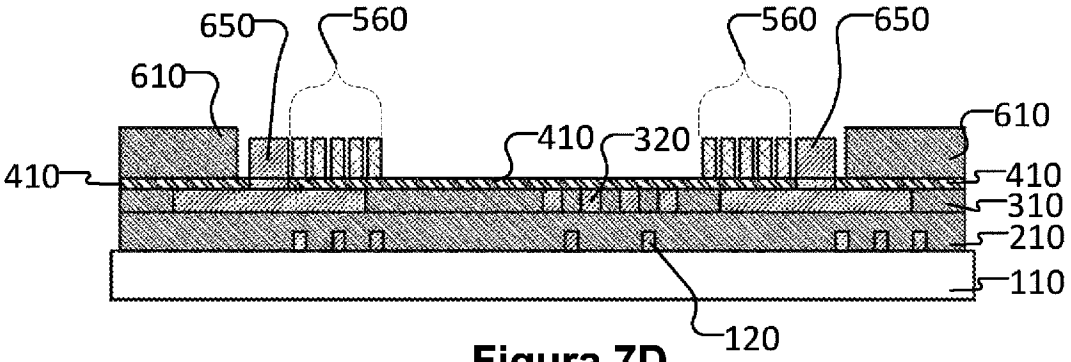

Figura 7D

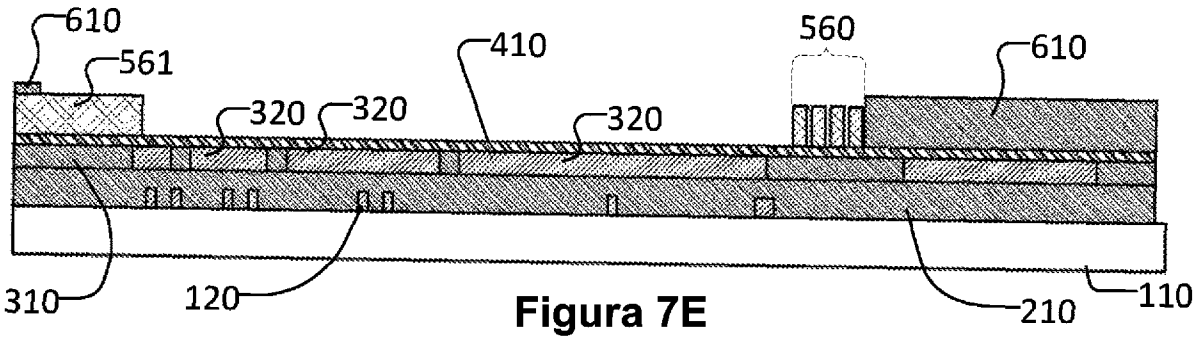

Figura 7E

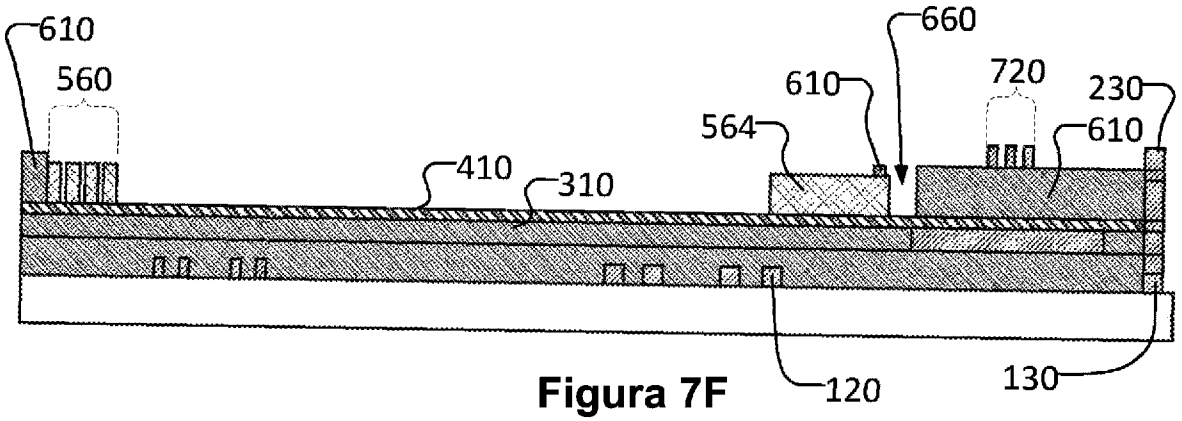

Figura 7F

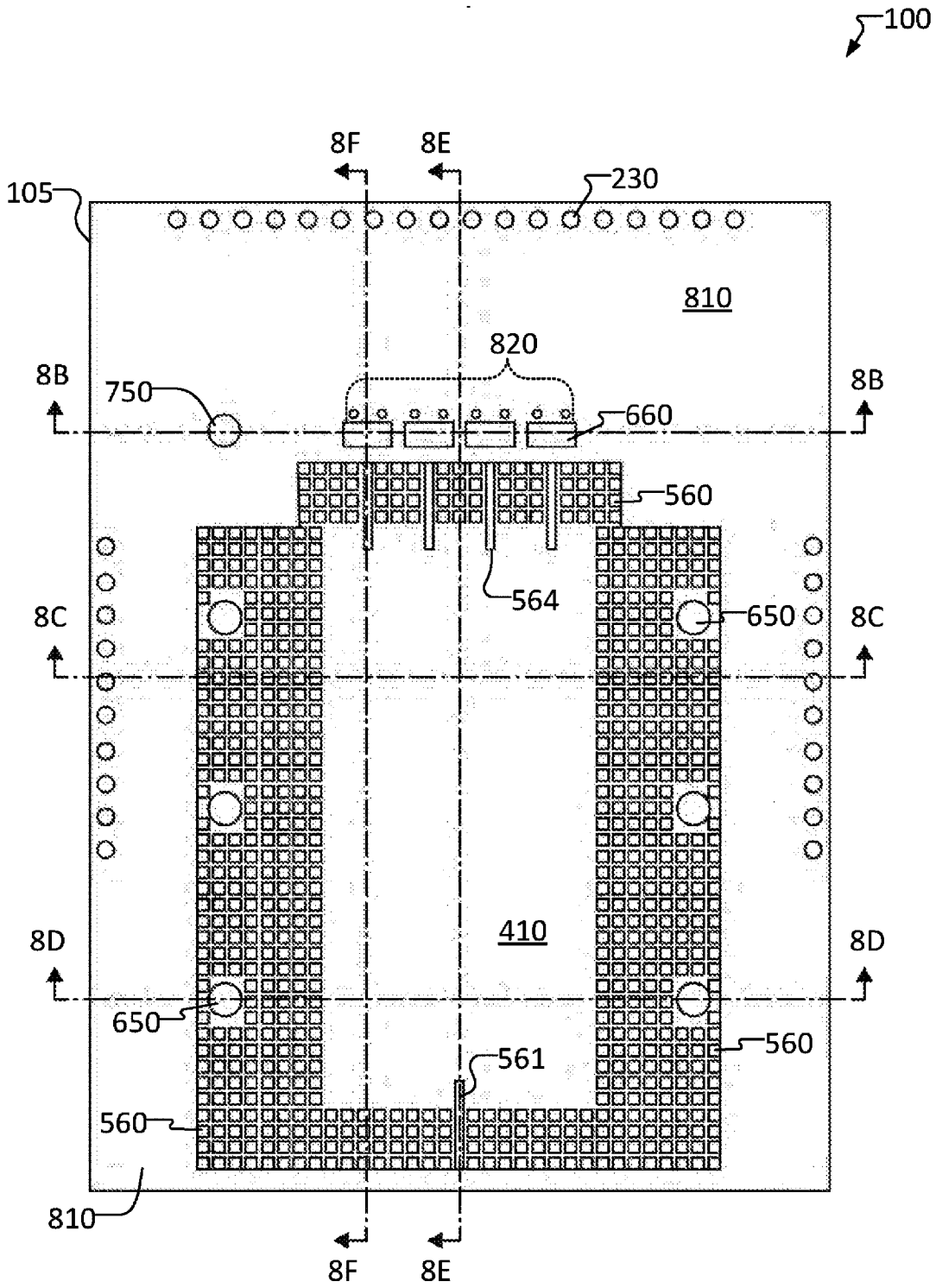
100
8F
8E
105
230
810
820
8B
750
660
8B
560
564
8C
650
8C
410
8D
8D
650
561
560
560
810
8F
8E

Figura 8A

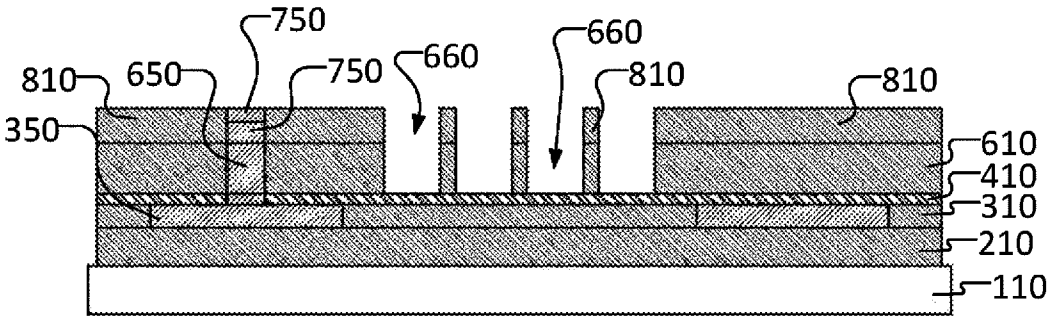

Figura 8B

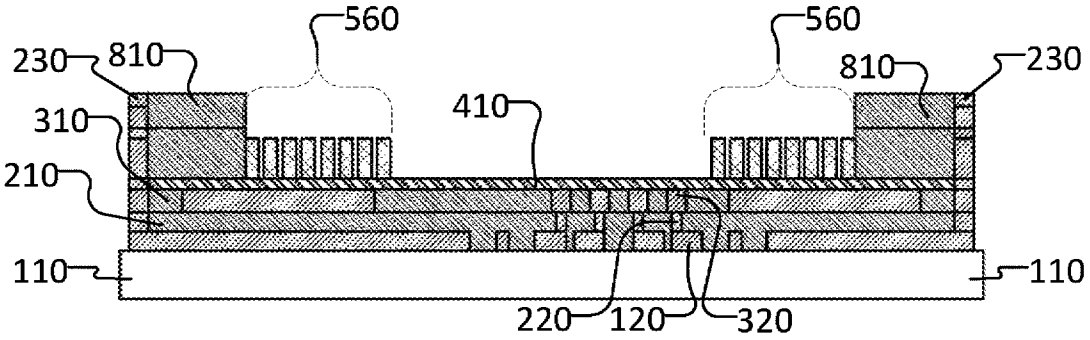

Figura 8C

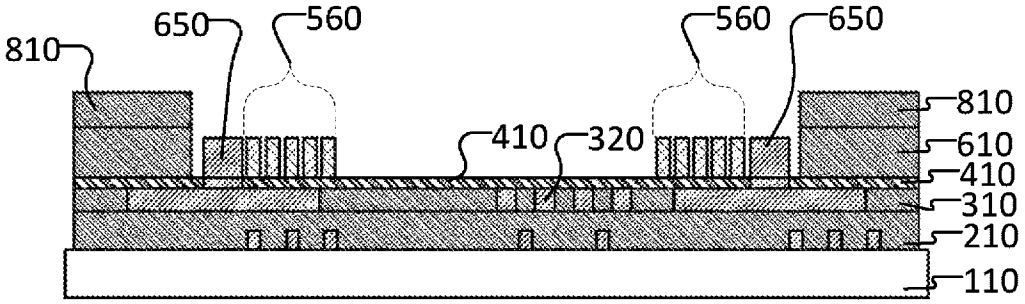

Figura 8D

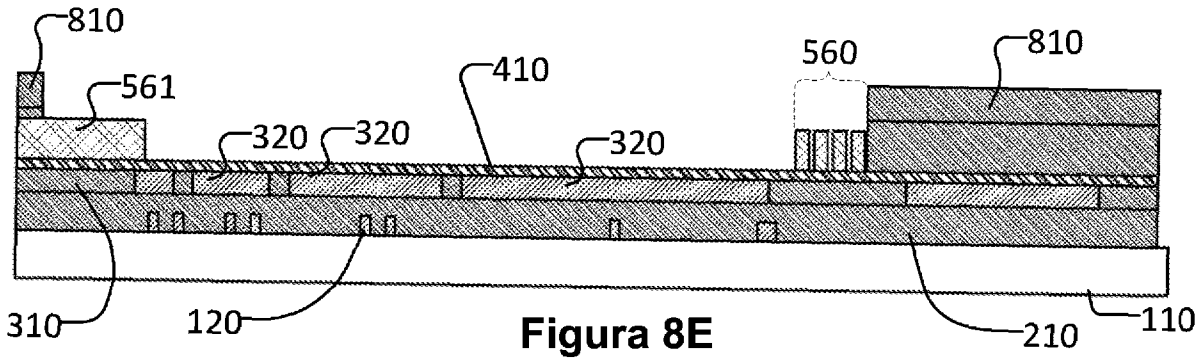

Figura 8E

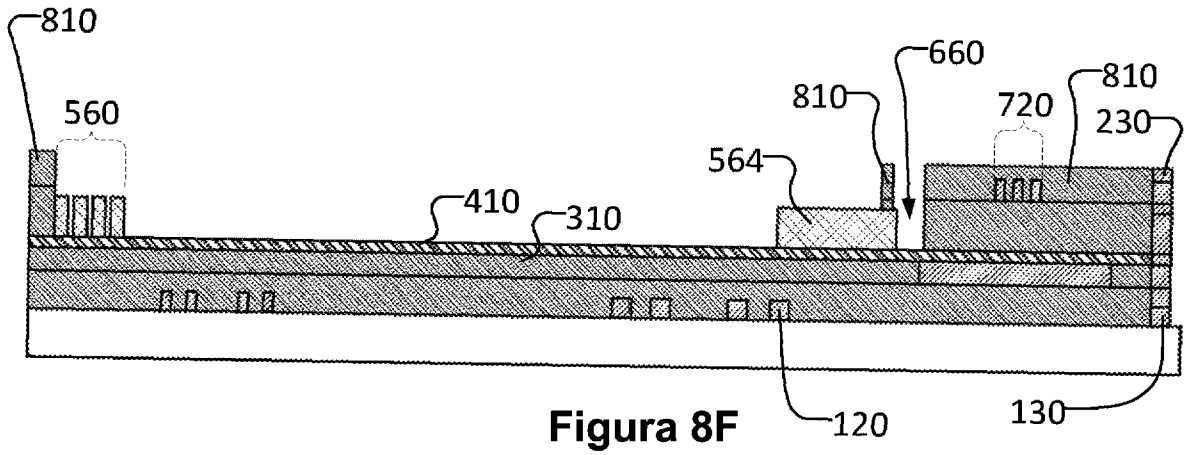

Figura 8F

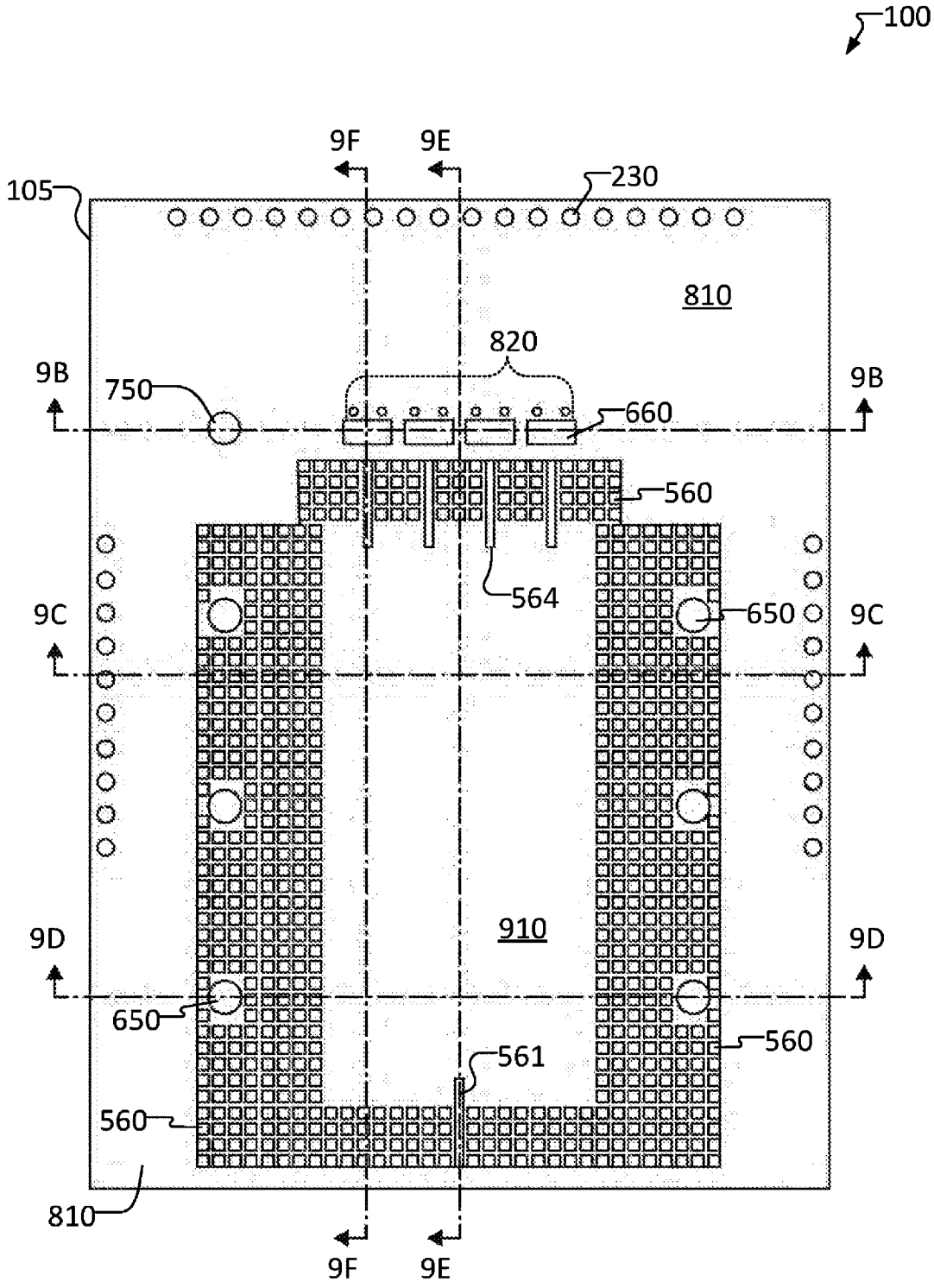
100
9F
9E
105
230
810
820
9B
750
660
9B
560
564
9C
650
9C
910
9D
9D
650
561
560
560
810
9F
9E

Figura 9A

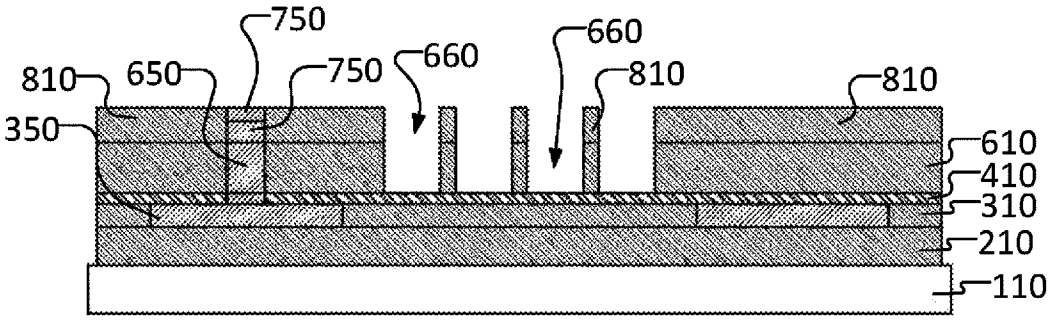

Figura 9B

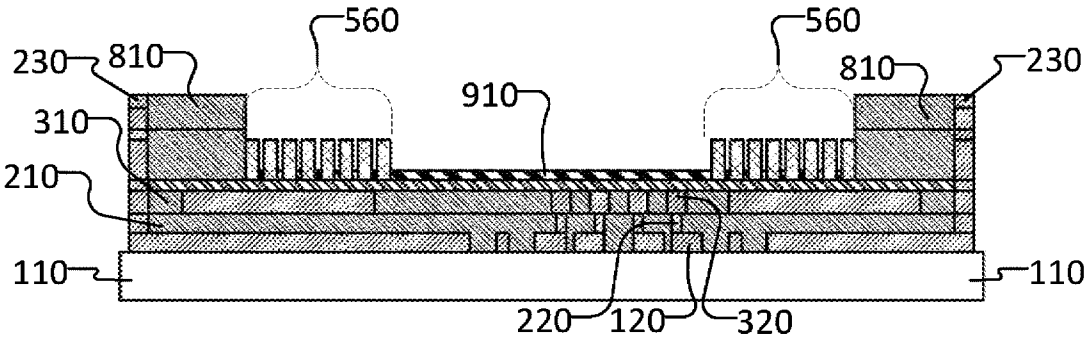

Figura 9C

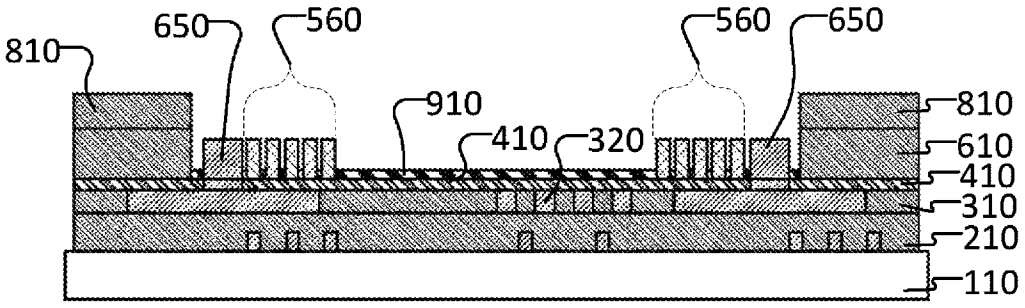

Figura 9D

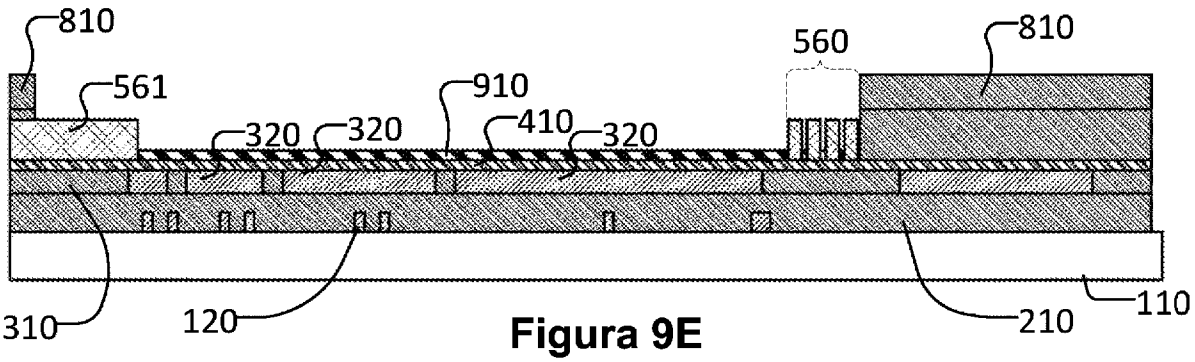

Figura 9E

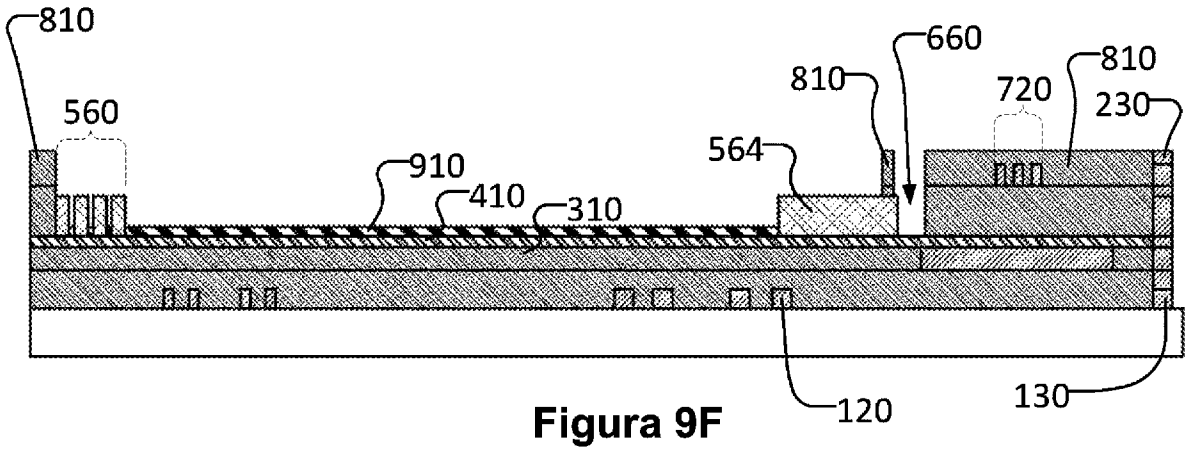

Figura 9F

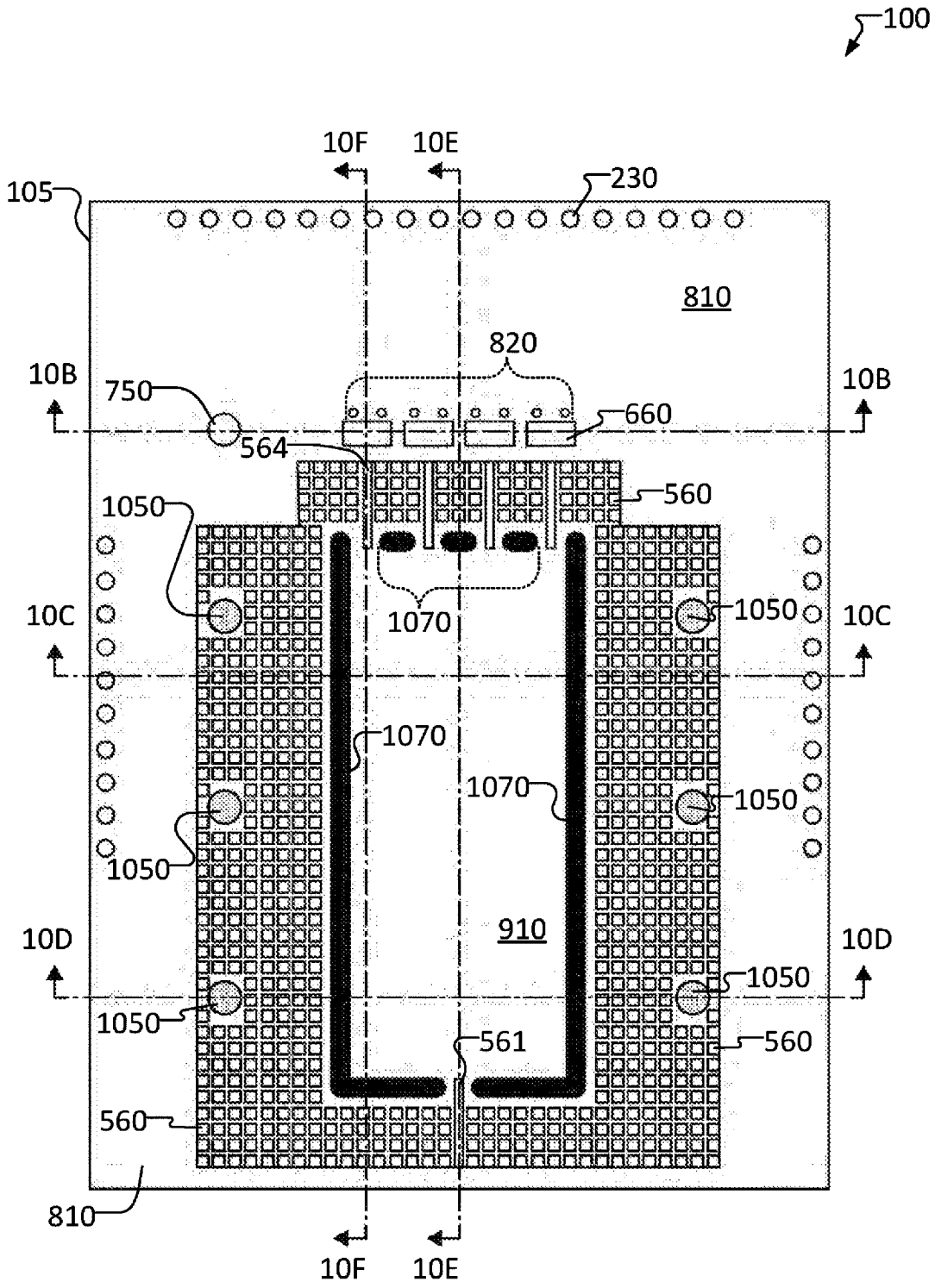
100
10F
10E
105
230
810
820
10B
750
660
564
560
1050
1070
10C
1050
1070
1070
1050
1050
910
10D
1050
1050
561
560
560
810
10F
10E

Figura 10A

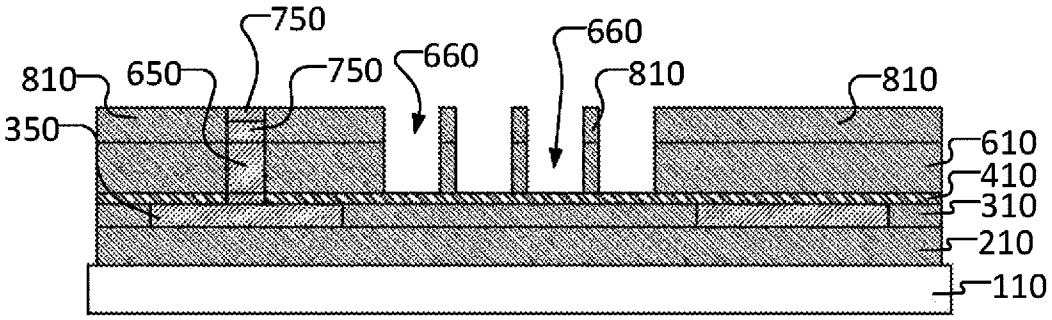

Figura 10B

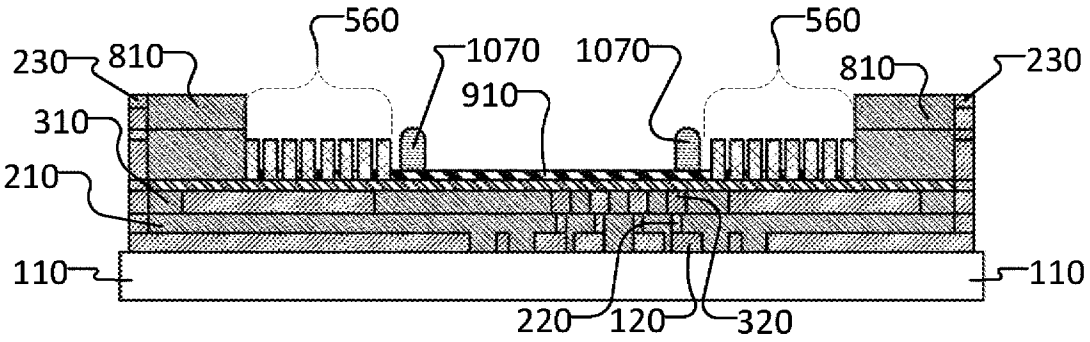

Figura 10C

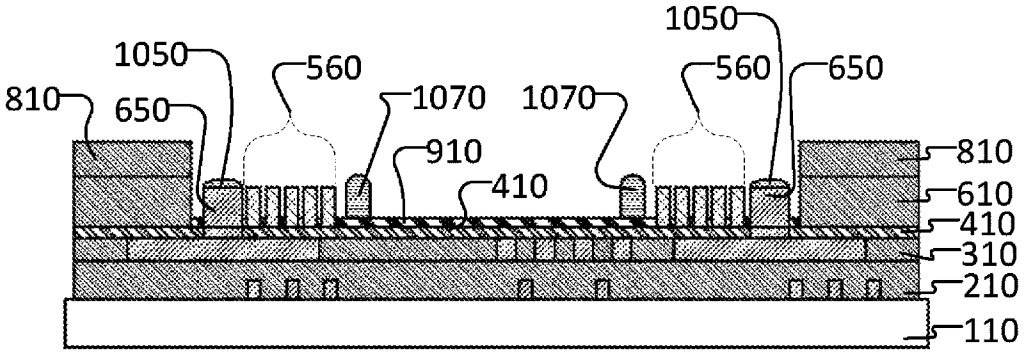

Figura 10D

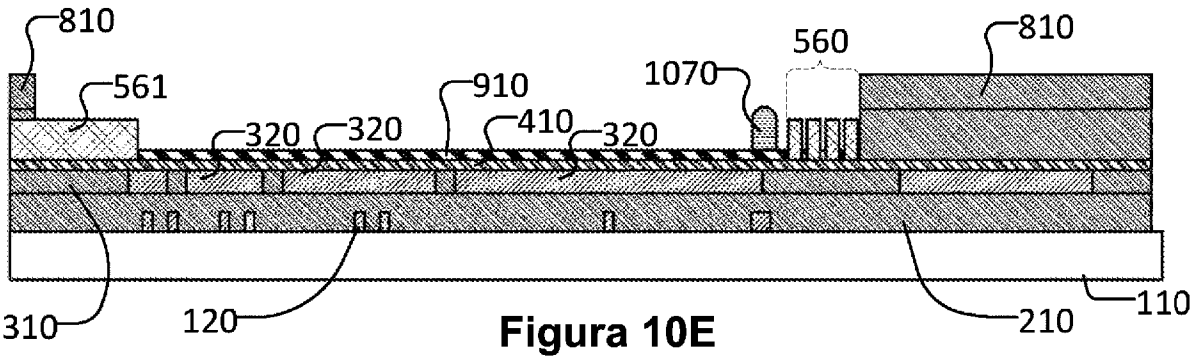

Figura 10E

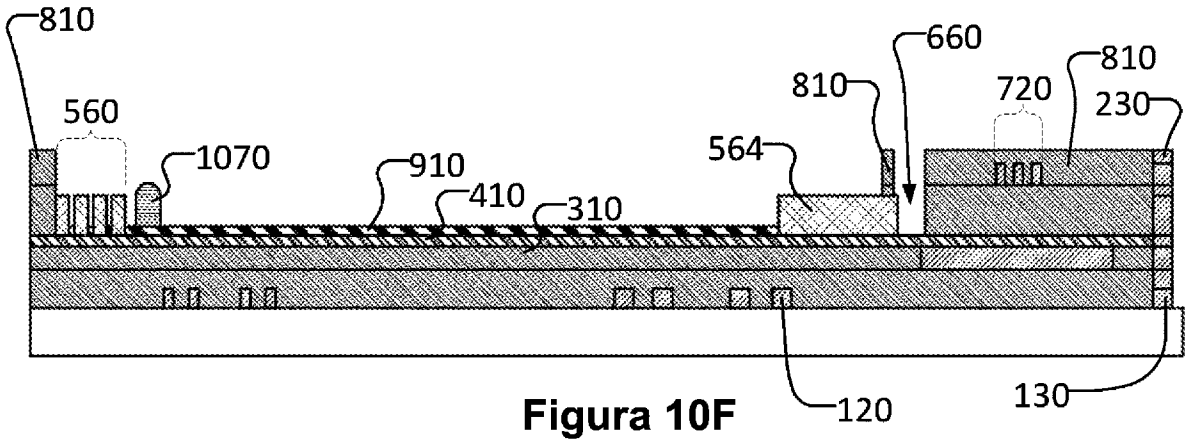

Figura 10F

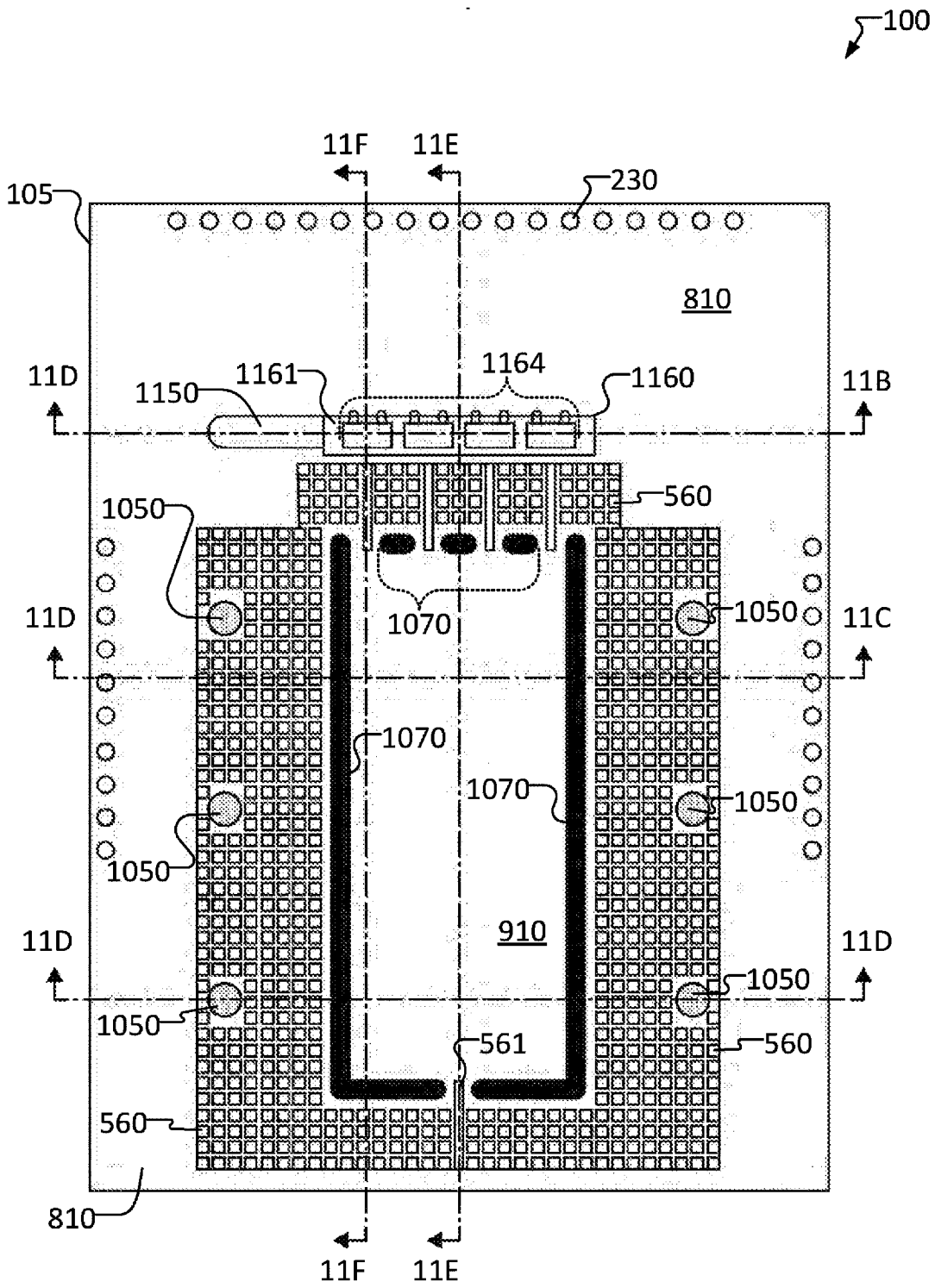
100
11F
11E
105
230
810
11D
1150
1161
1164
1160
11B
560
1050
1070
11C
910
561
810

Figura 11A

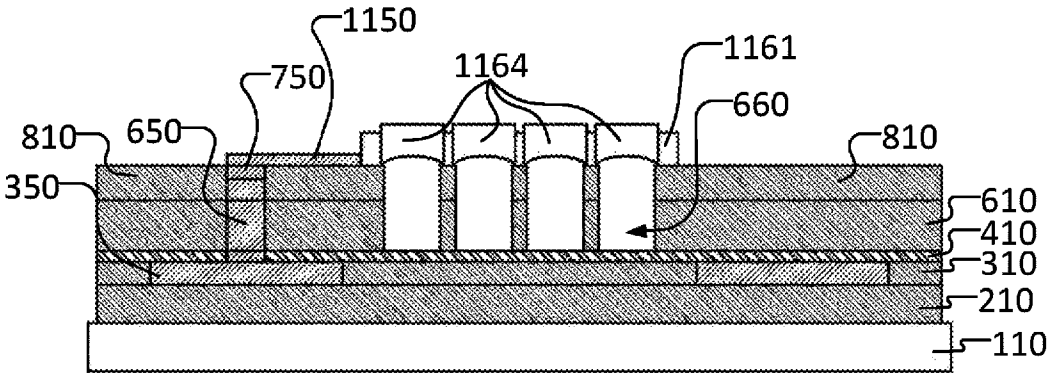

Figura 11B

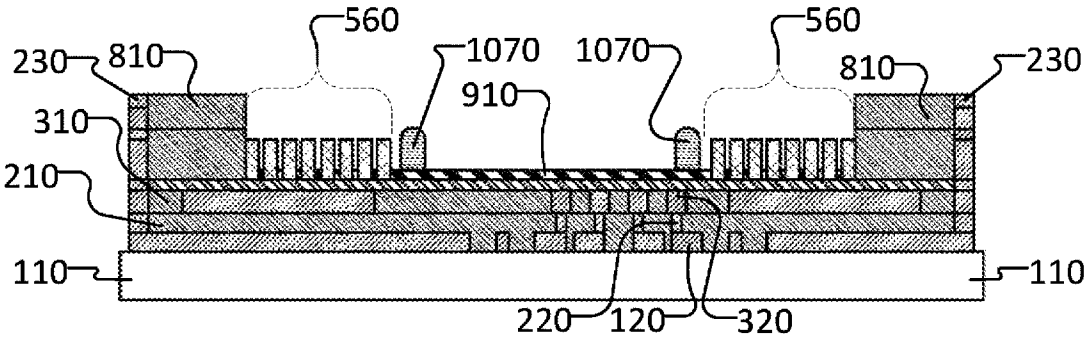

Figura 11C

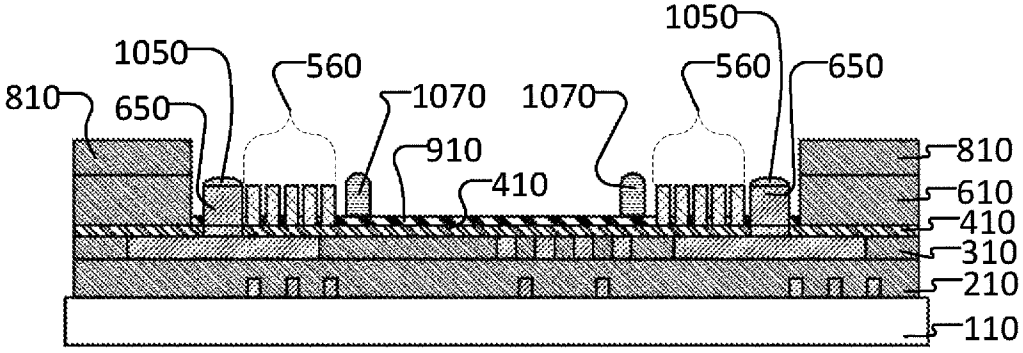

Figura 11D

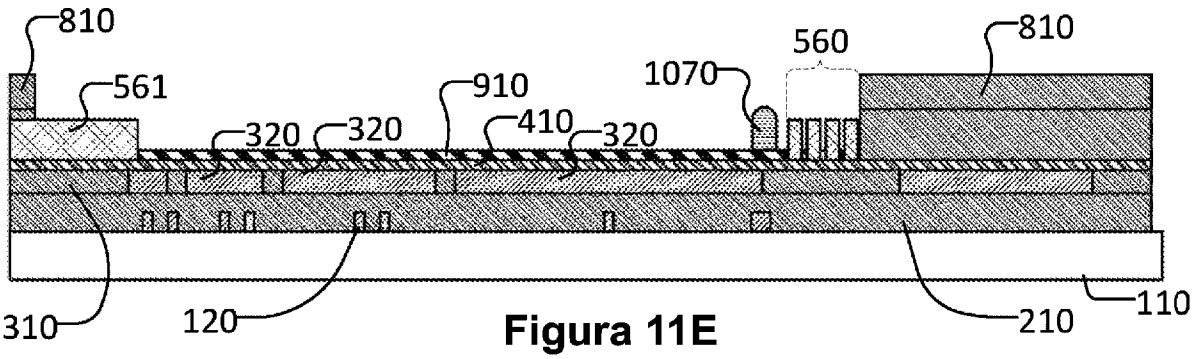

Figura 11E

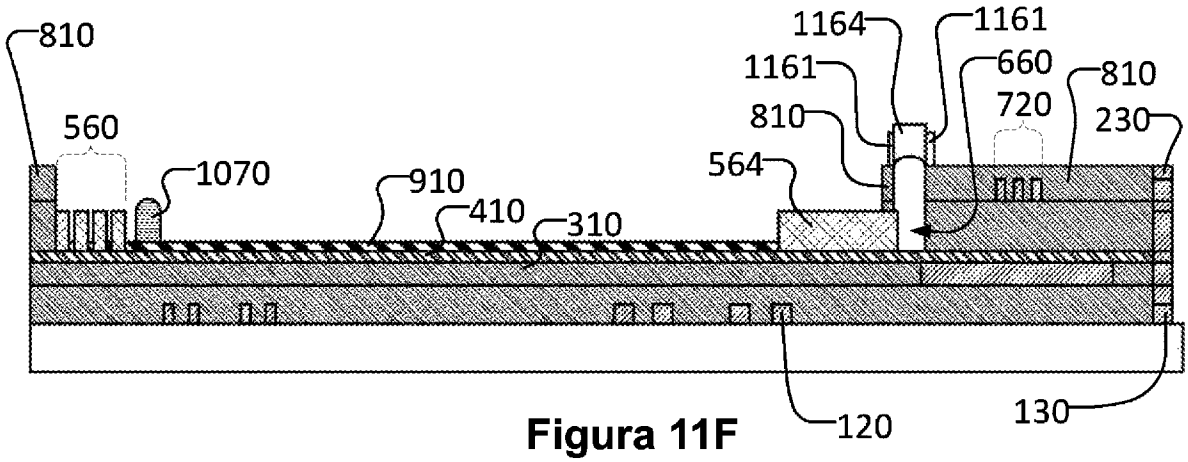

Figura 11F

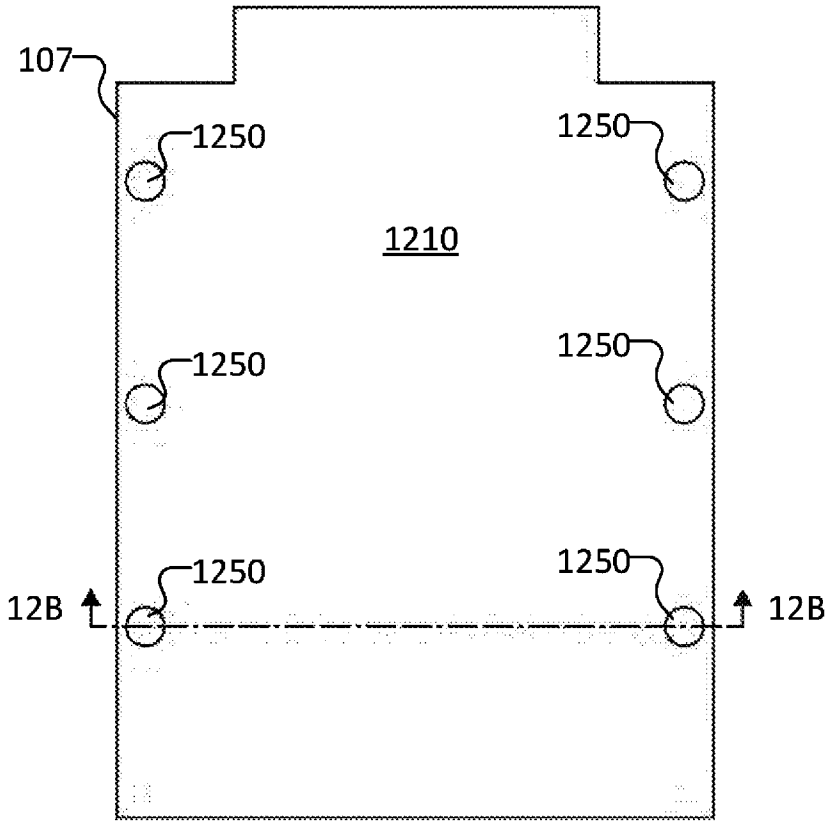

Figura 12A

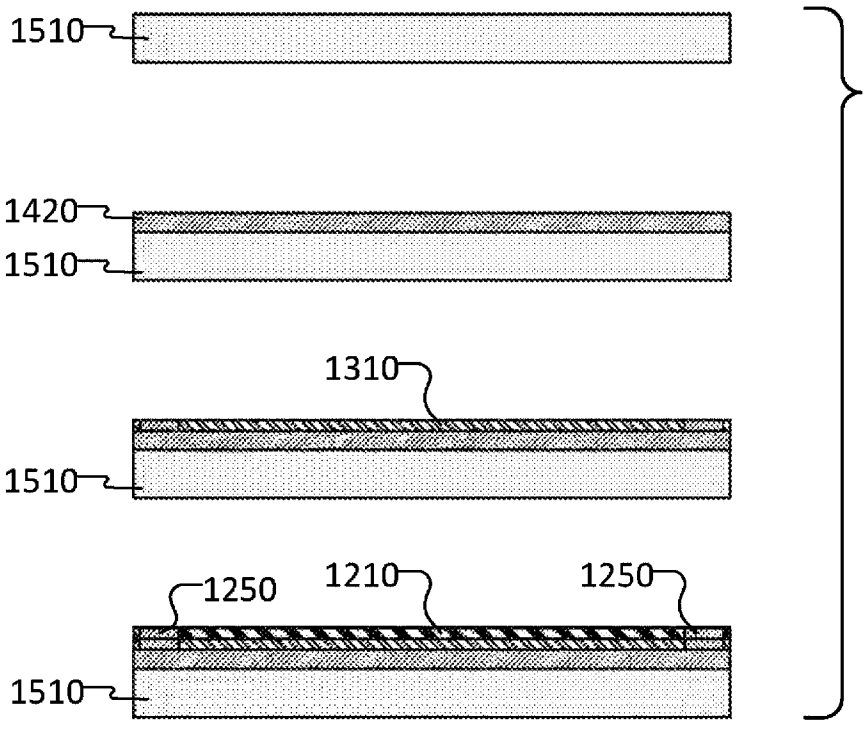

Figura 12B

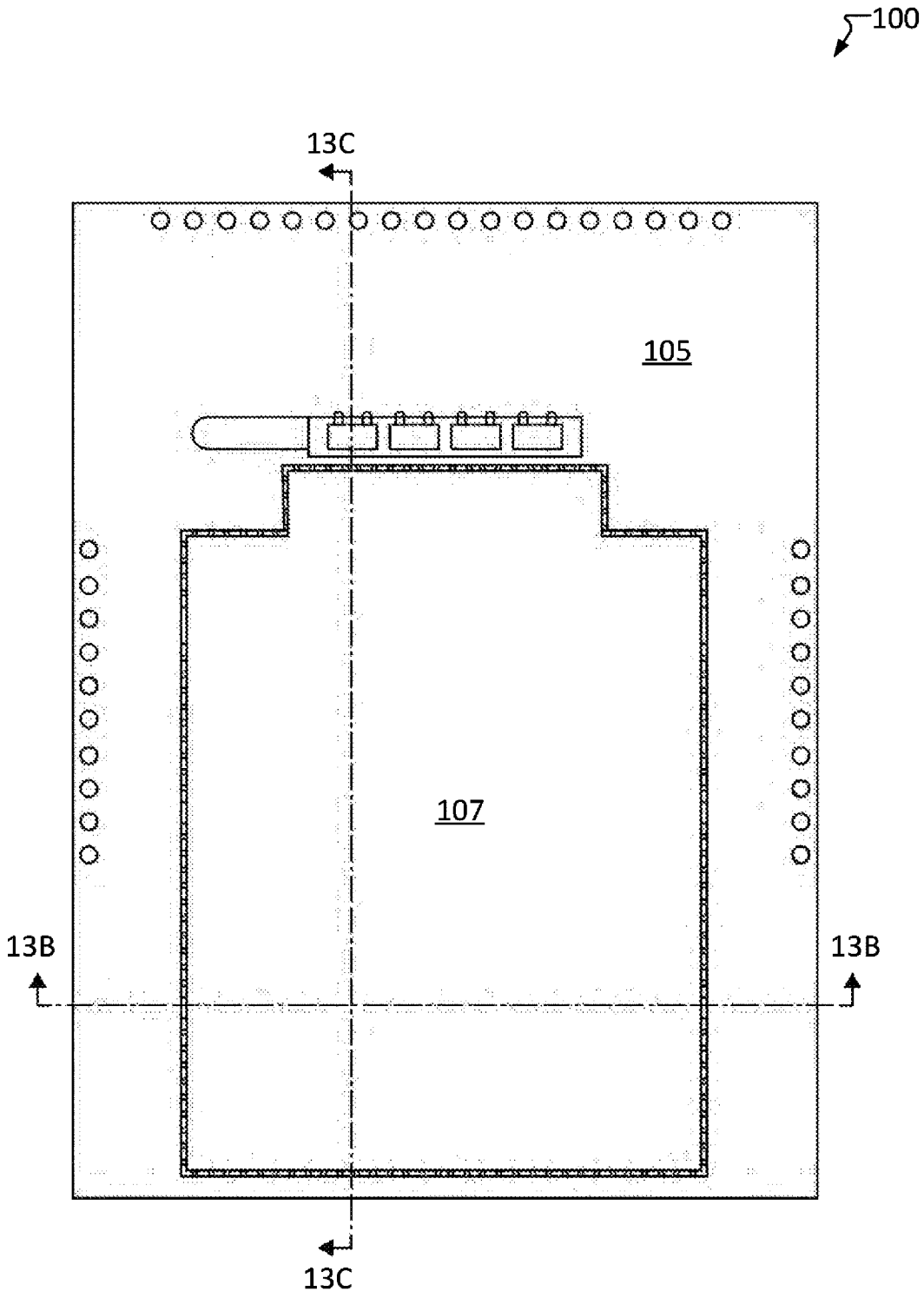

Figura 13A

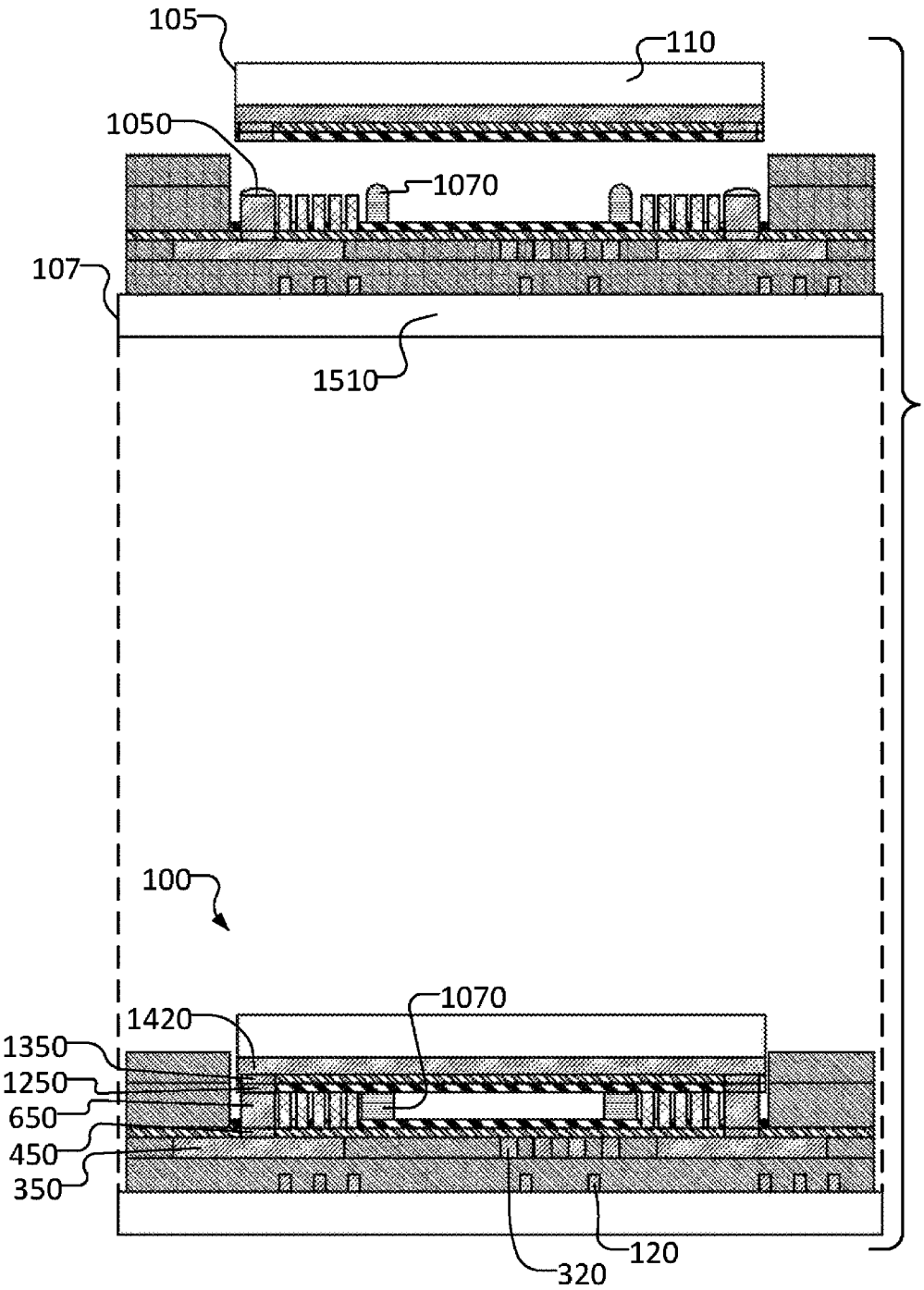
105
110
1050
1070
107
1510
100
1420
1070
1350
1250
650
450
350
320
120

Figura 13B

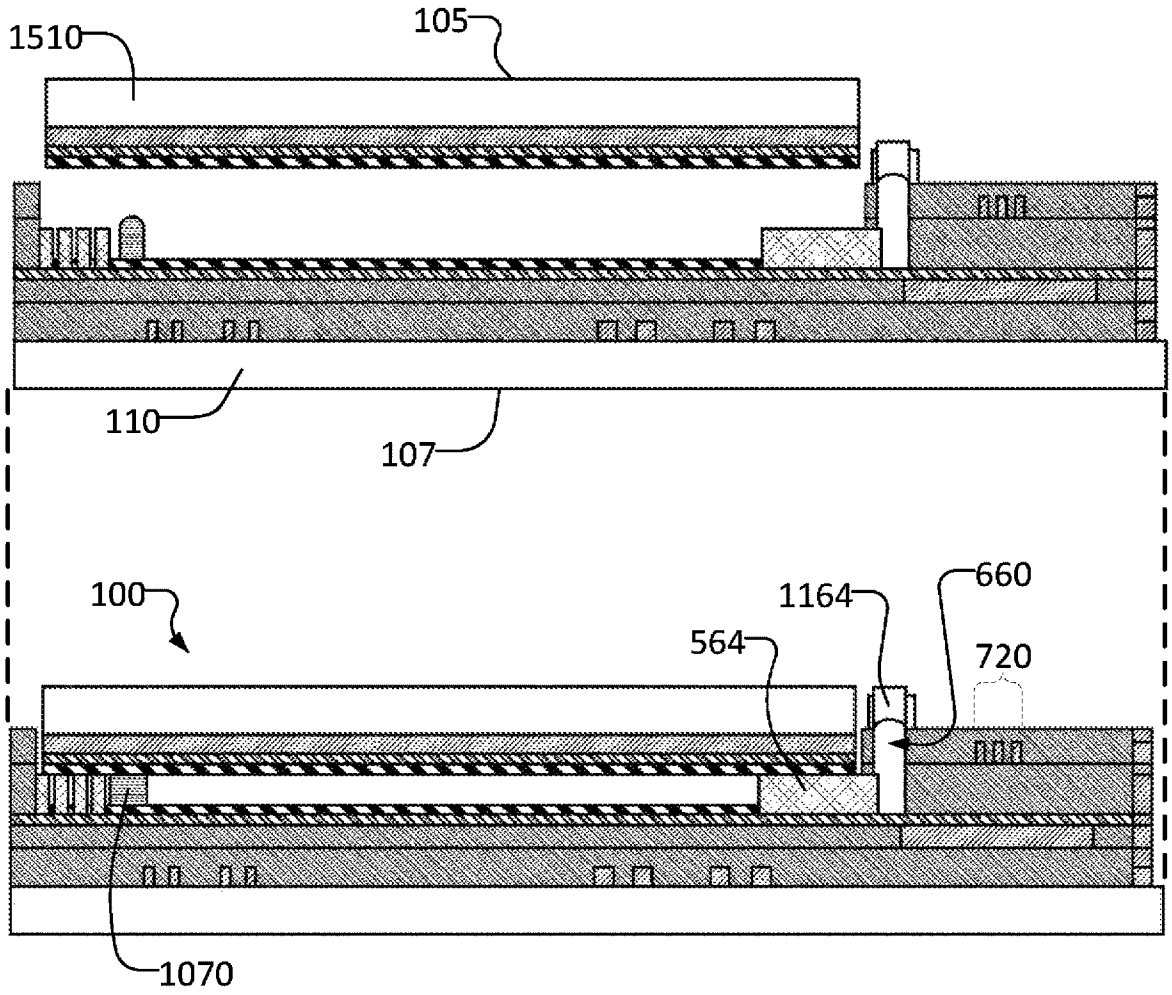

Figura 13C

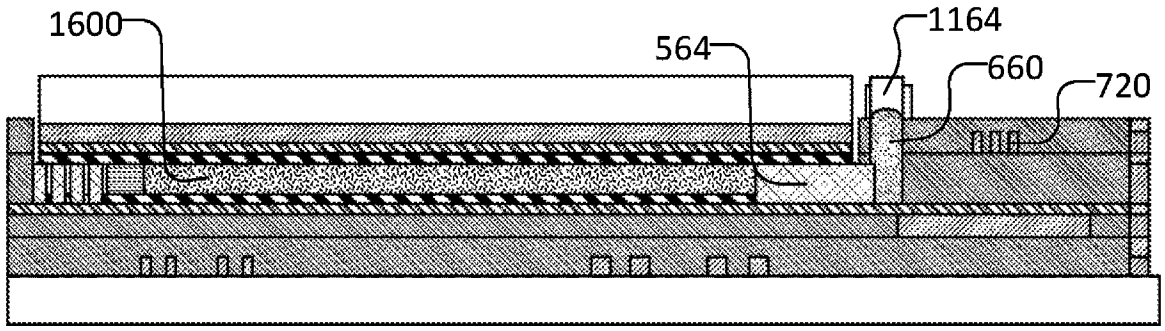

Figura 14A

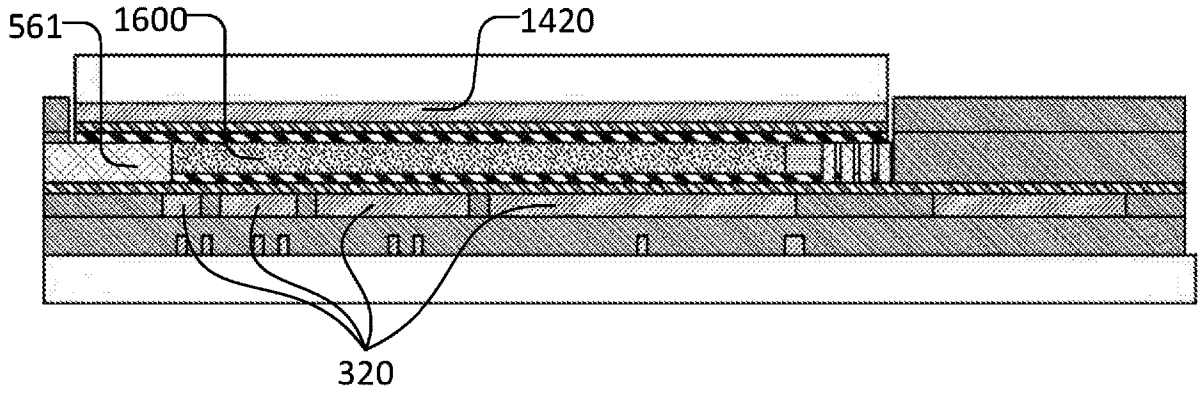

Figura 14B

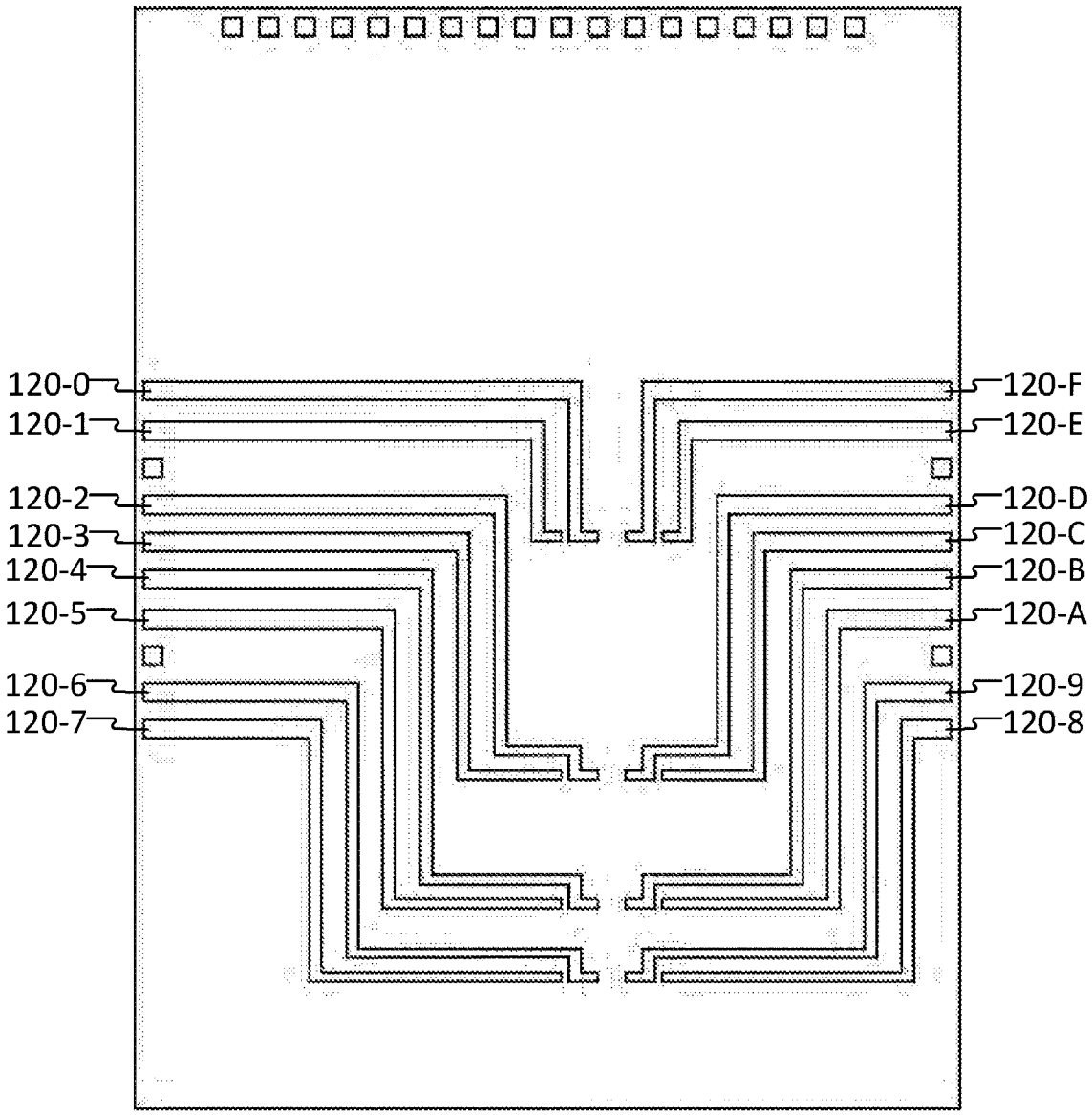
120-0
120-1
120-2
120-3
120-4
120-5
120-6
120-7
120-F
120-E
120-D
120-C
120-B
120-A
120-9
120-8

Figura 15

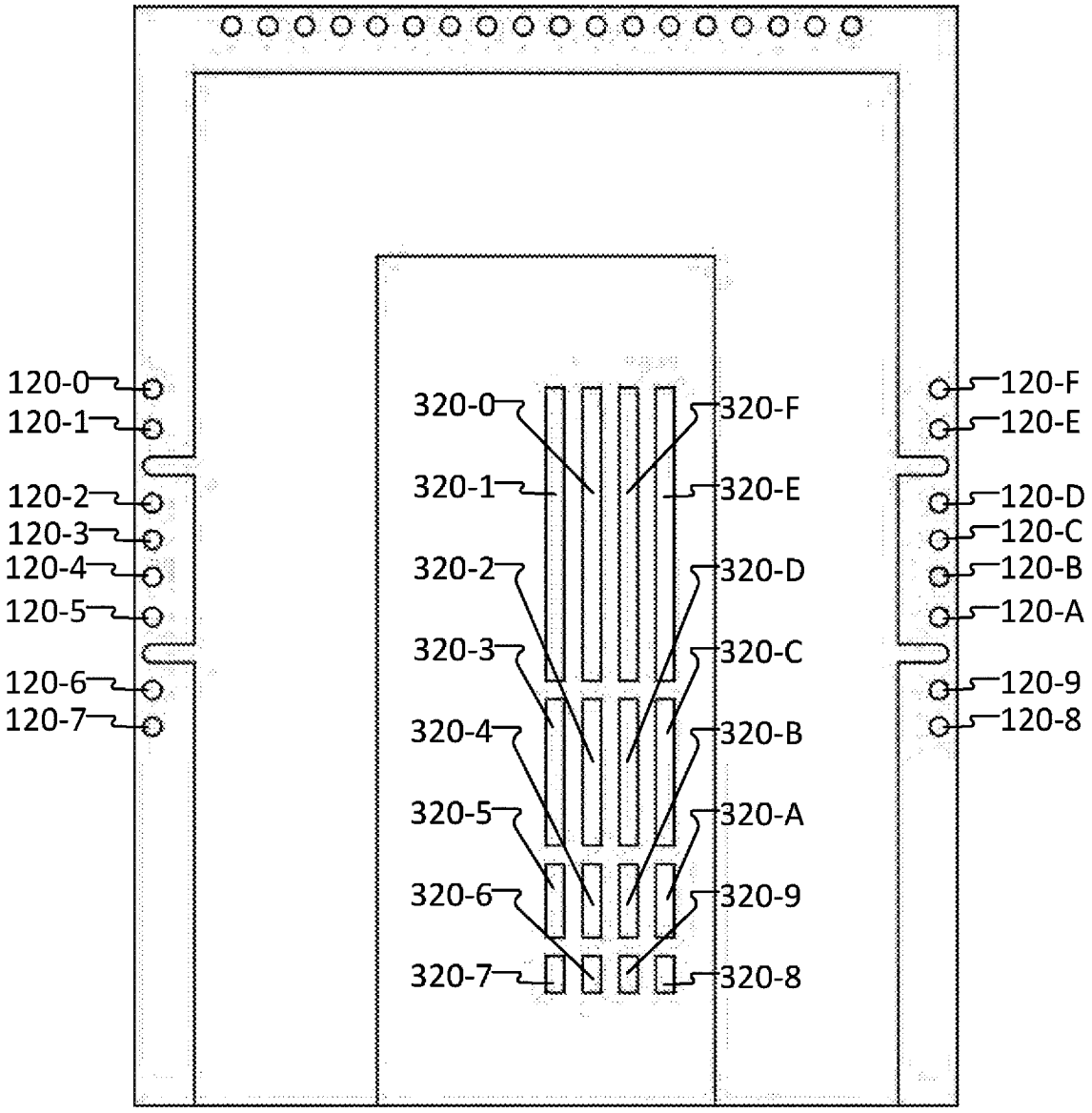
120-0
120-1
120-2
120-3
120-4
120-5
120-6
120-7
320-0
320-1
320-2
320-3
320-4
320-5
320-6
320-7
320-F
320-E
320-D
320-C
320-B
320-A
320-9
320-8
120-F
120-E
120-D
120-C
120-B
120-A
120-9
120-8

Figura 16

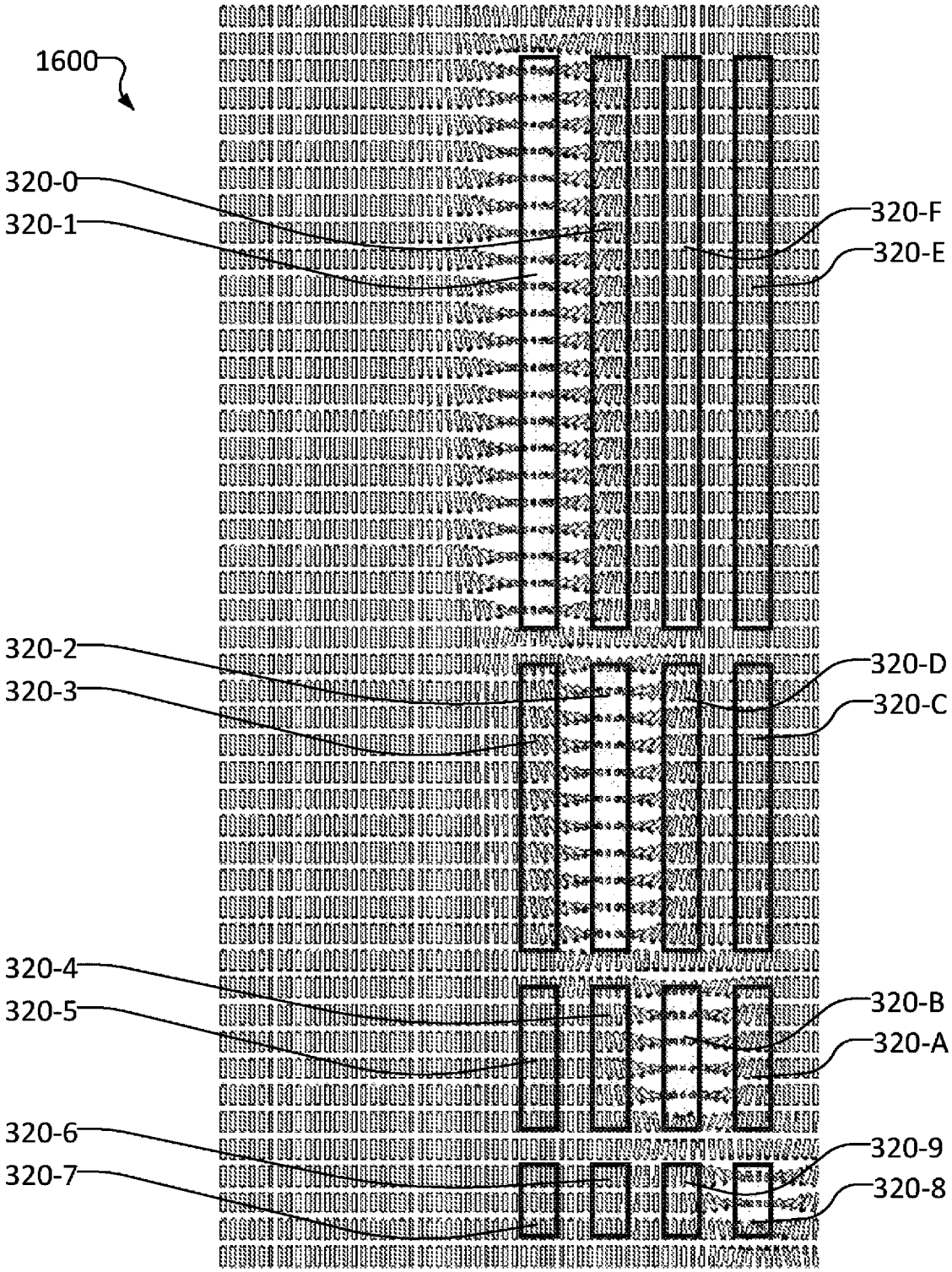
1600
320-0
320-1
320-F
320-E
320-2
320-3
320-D
320-C
320-4
320-5
320-B
320-A
320-6
320-7
320-9
320-8

Figura 17

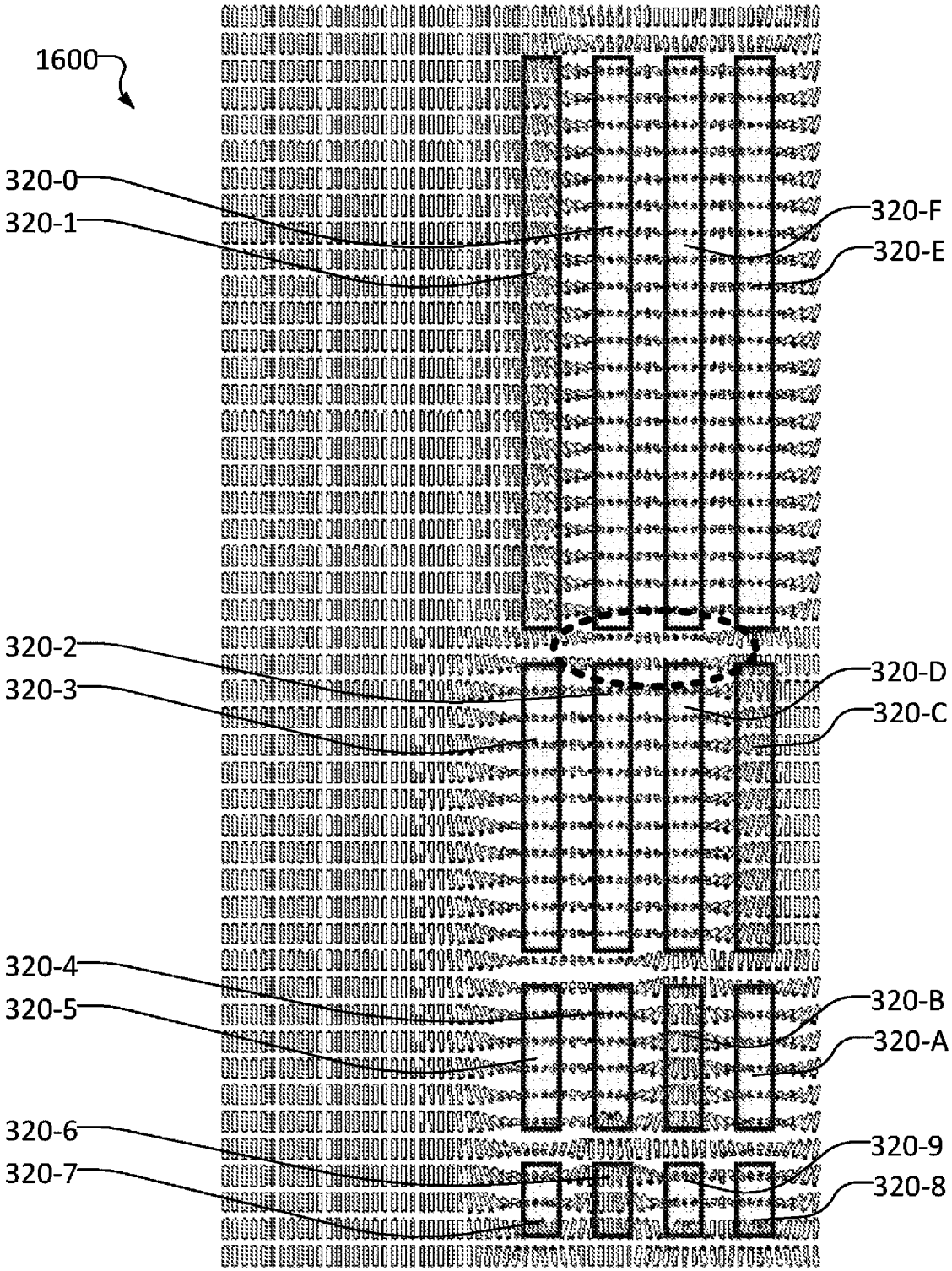
1600
320-0
320-1
320-F
320-E
320-2
320-3
320-D
320-C
320-4
320-5
320-B
320-A
320-6
320-7
320-9
320-8

Figura 18

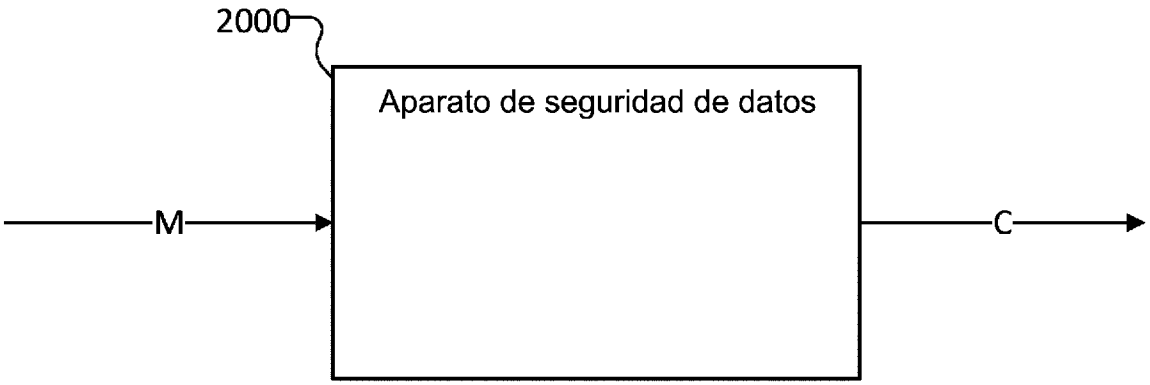

Figura 19A

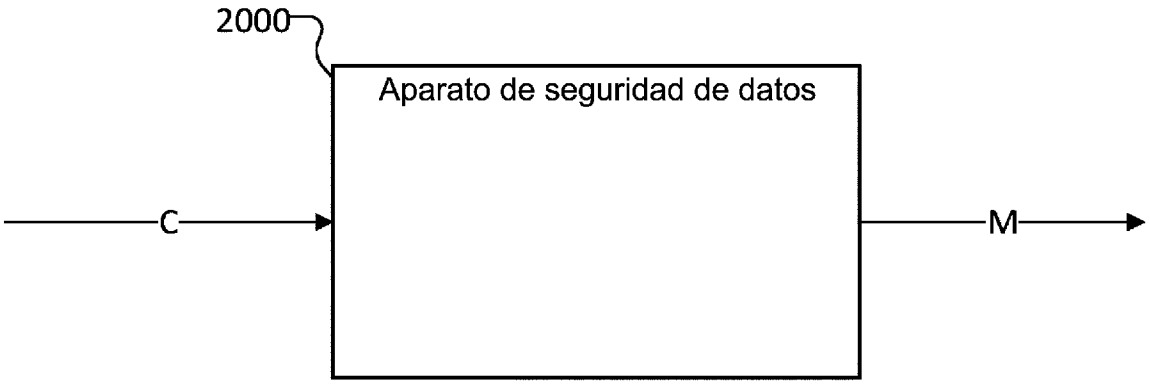

Figura 19B

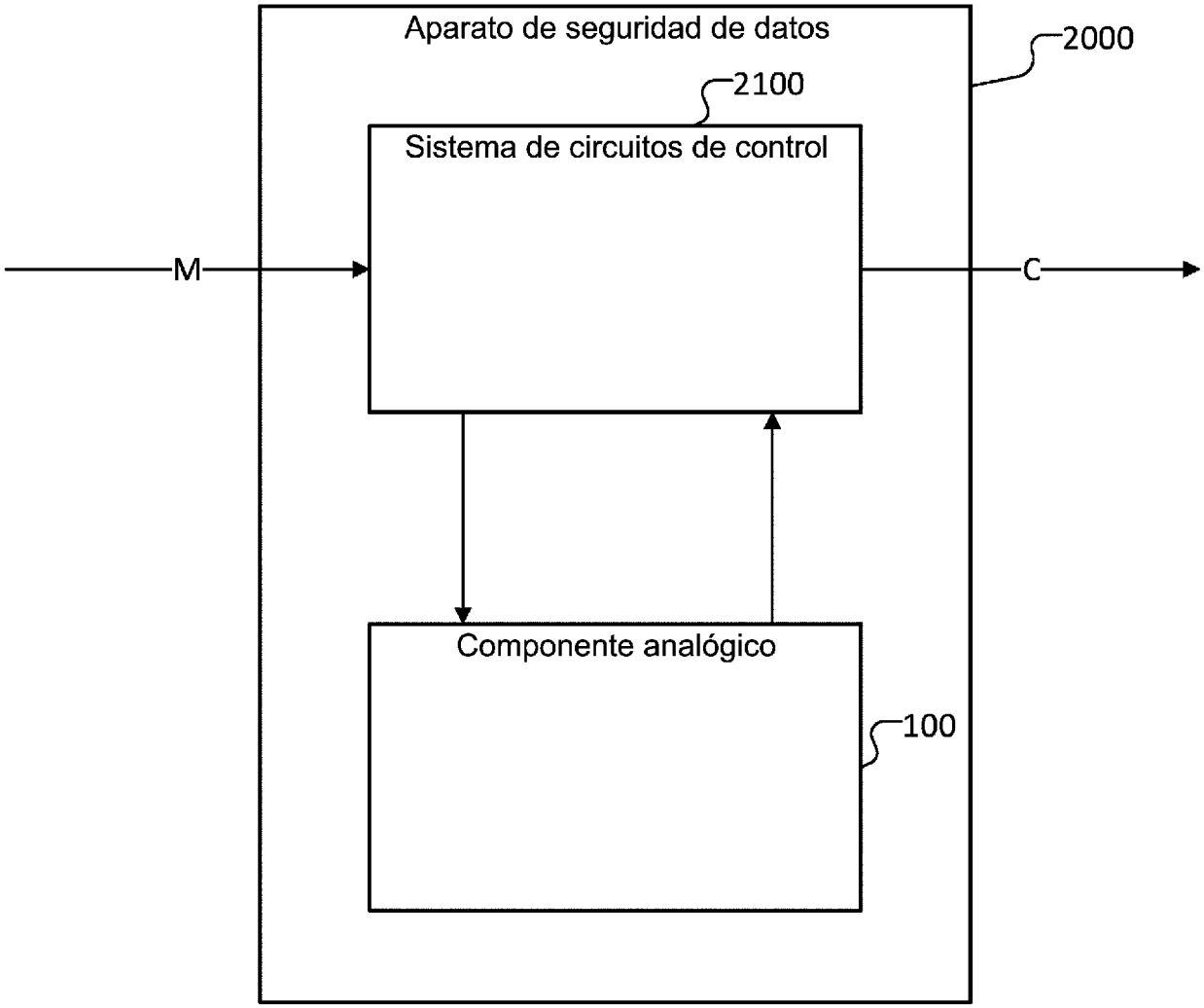
Aparato de seguridad de datos
2000
2100
Sistema de circuitos de control
M
C
Componente analógico
100

Figura 20

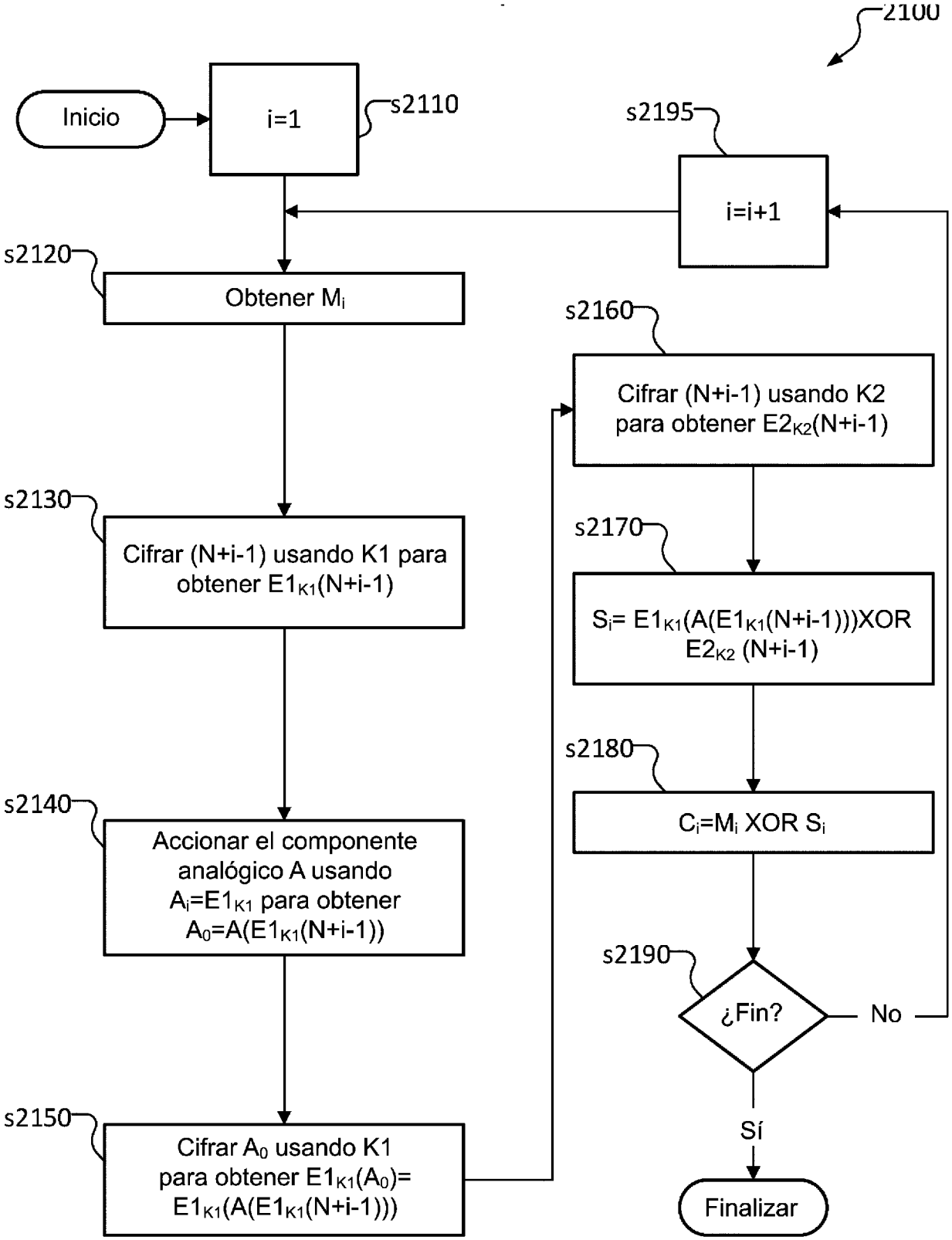
2100
Inicio
i=1
s2110
s2195
i=i+1
s2120
Obtener M_i
s2160
Cifrar (N+i-1) usando K2 para obtener $E2_{K2}(N+i-1)$
s2130
Cifrar (N+i-1) usando K1 para obtener $E1_{K1}(N+i-1)$
s2170
$S_i= E1_{K1}(A(E1_{K1}(N+i-1)))XOR E2_{K2}(N+i-1)$
s2180
$C_i=M_i$ XOR S_i
s2140
Accionar el componente analógico A usando $A_i=E1_{K1}$ para obtener $A_0=A(E1_{K1}(N+i-1))$
s2190
¿Fin?
No
Sí
s2150
Cifrar A_0 usando K1 para obtener $E1_{K1}(A_0)= E1_{K1}(A(E1_{K1}(N+i-1)))$
Finalizar

Figura 21

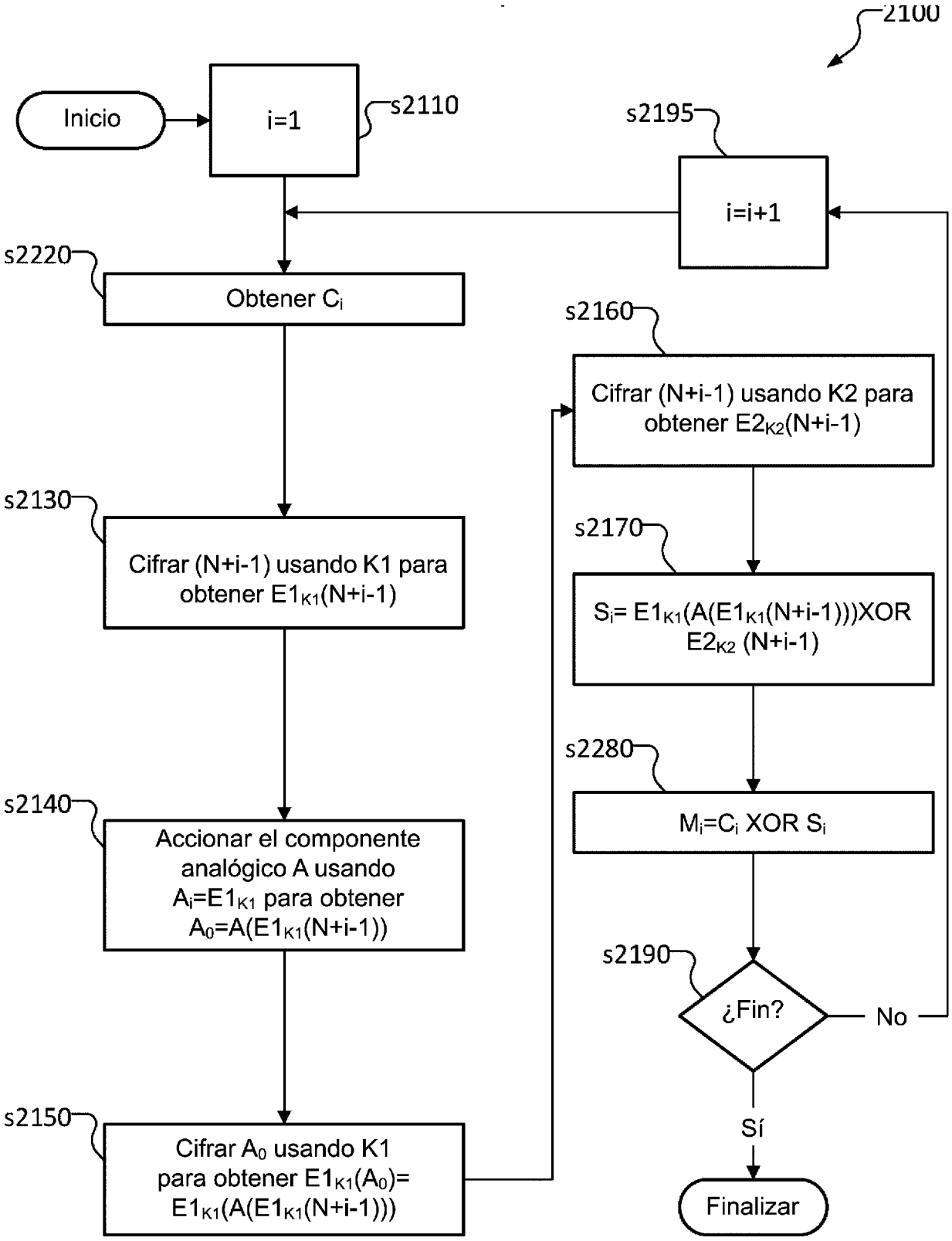
2100
Inicio
i=1
s2110
s2195
i=i+1
s2220
Obtener C_i
s2160
Cifrar (N+i-1) usando K2 para obtener $E2_{K2}(N+i-1)$
s2130
Cifrar (N+i-1) usando K1 para obtener $E1_{K1}(N+i-1)$
s2170
$S_i= E1_{K1}(A(E1_{K1}(N+i-1)))XOR E2_{K2}(N+i-1)$
s2280
$M_i=C_i$ XOR S_i
s2140
Accionar el componente analógico A usando $A_i=E1_{K1}$ para obtener $A_0=A(E1_{K1}(N+i-1))$
s2190
¿Fin?
No
Sí
s2150
Cifrar A_0 usando K1 para obtener $E1_{K1}(A_0)= E1_{K1}(A(E1_{K1}(N+i-1)))$
Finalizar

Figura 22

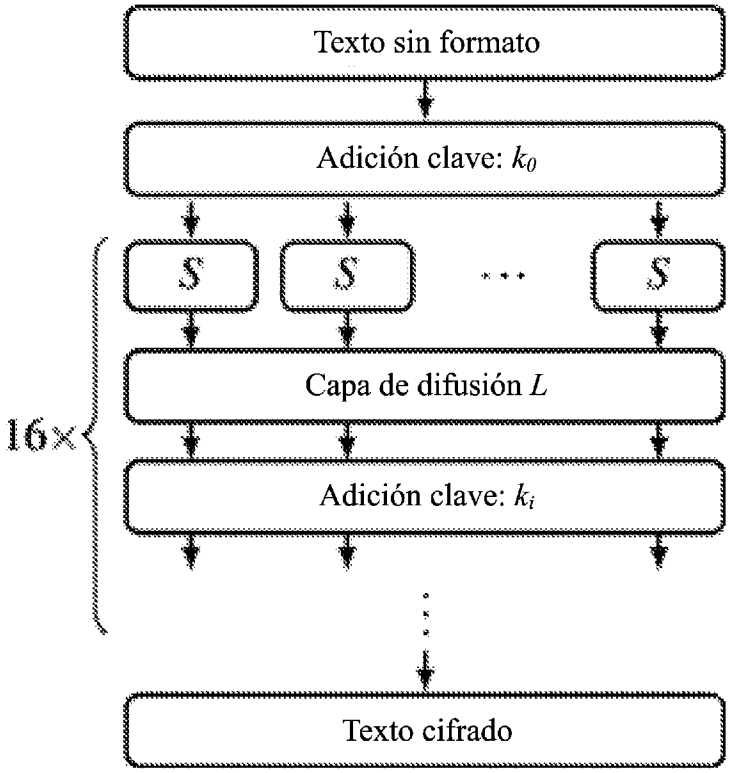
Texto sin formato
Adición clave: k_0
S
S
S
Capa de difusión L
16×
Adición clave: k_i
Texto cifrado

Figura 23

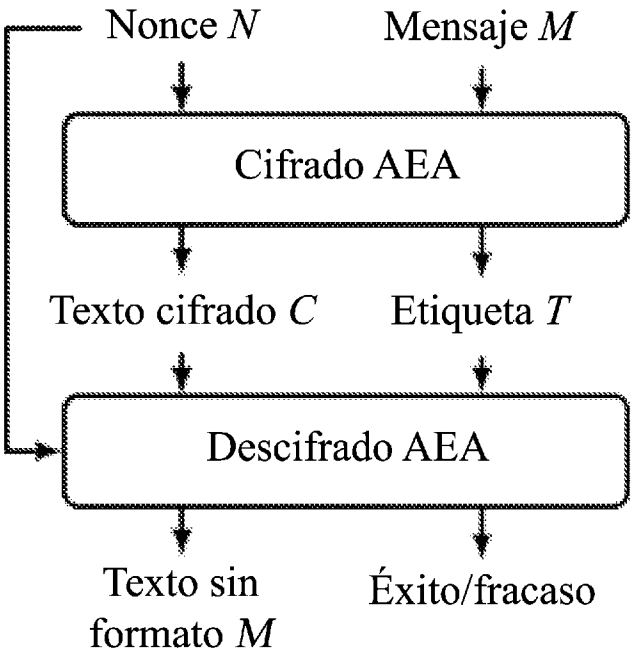

Figura 24

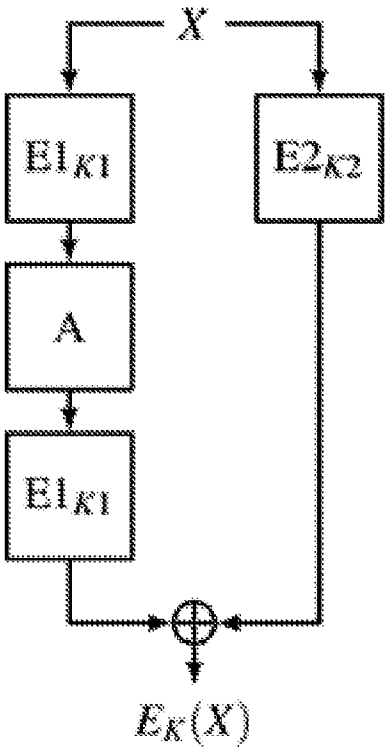

Figura 25

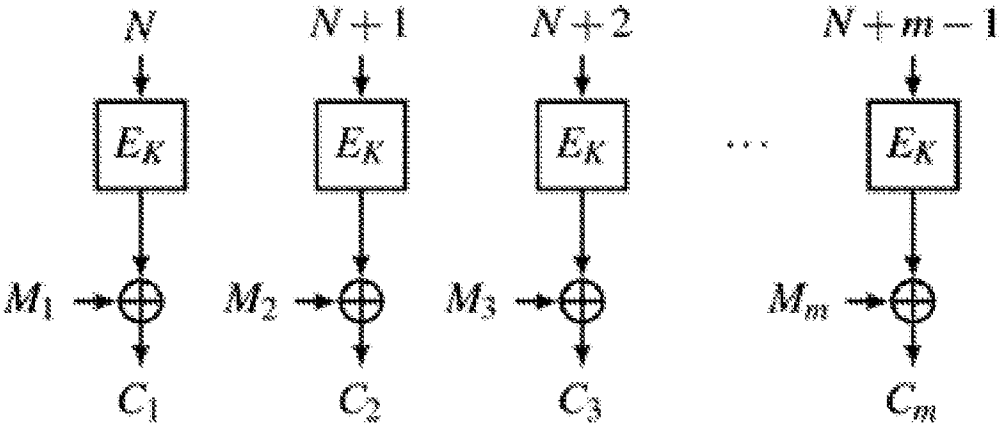

Figura 26

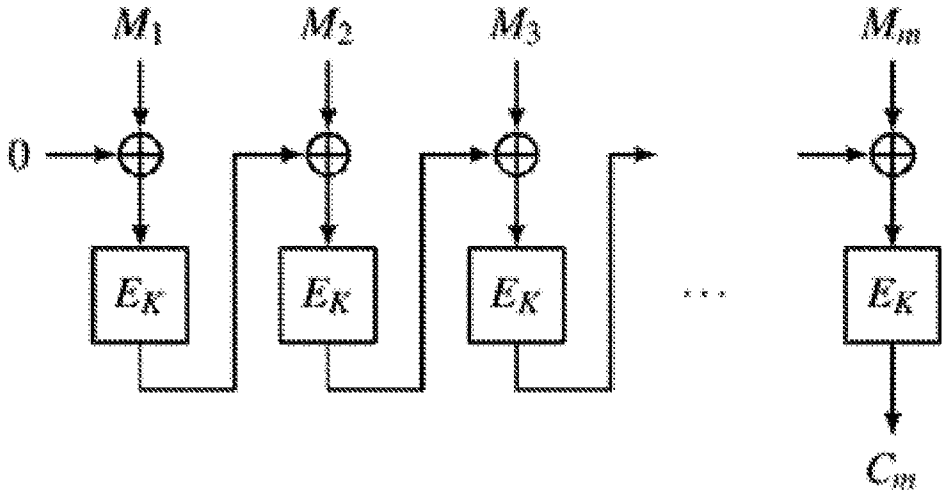

Figura 27

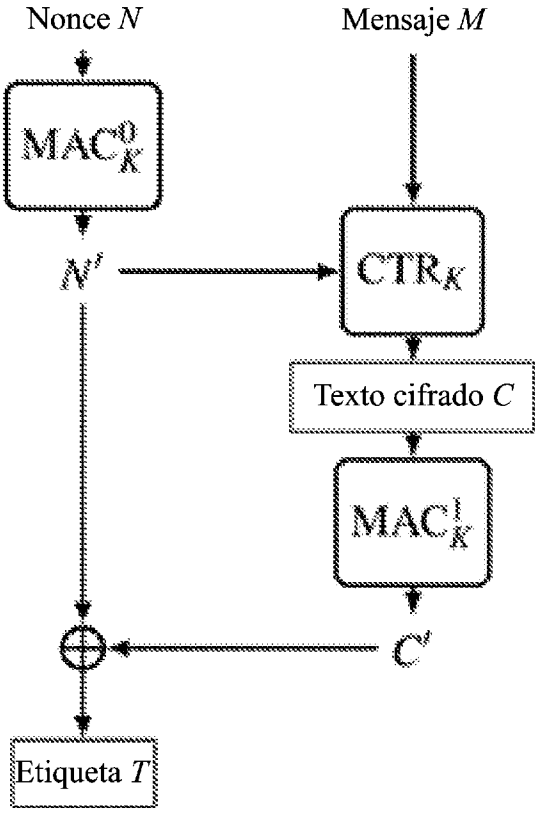

Figura 28