(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 721 480**

(51) Int. CI.:

G06F 21/83 (2013.01)
G06F 3/02 (2006.01)
G06F 3/023 (2006.01)
H03M 11/02 (2006.01)
H03M 11/04 (2006.01)
H03M 11/20 (2006.01)
H03M 11/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.10.2012 PCT/EP2012/071189**

(87) Fecha y número de publicación internacional: **02.05.2013 WO13060801**

(96) Fecha de presentación y número de la solicitud europea: **25.10.2012 E 12777920 (5)**

(97) Fecha y número de publicación de la concesión europea: **23.01.2019 EP 2771976**

(54) Título: **Procedimiento y dispositivo para gestionar una matriz de teclas, programa informático y medios de almacenamiento correspondientes**

(30) Prioridad:

28.10.2011 FR 1159798

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.07.2019

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

BELLAHCENE, MOHAMMED;
BENOIT, OLIVIER y
DELORME, JEAN-JACQUES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivo para gestionar una matriz de teclas, programa informático y medios de almacenamiento correspondientes

1. Sector de la invención

El sector de la invención es el de los teclados matriciales, es decir, los teclados que comprenden una matriz de teclas que permiten al usuario introducir caracteres (letras, números, símbolos, etc.).

De manera más precisa, la invención se refiere a una técnica de gestión segura de dicha matriz de teclas mediante un dispositivo (por ejemplo, un procesador), para determinar la tecla o teclas pulsadas por el usuario. Esta técnica también se conoce como “rutina de escaneo del teclado” (o “keyboard scan routine”, en inglés).

La invención se aplica en particular, pero no exclusivamente, al teclado de un terminal de pago para el pago de compras de bienes y servicios. En este caso, el teclado permite la introducción de los importes de las transacciones por parte del vendedor, así como la introducción de los PIN (códigos PIN, “Número de Identificación Personal”, Personal Identity Number, en inglés) por parte de los clientes.

La invención no se limita a un tipo particular de teclado, y se aplica cualquiera que sea el número y la naturaleza de las teclas del teclado (teclas numéricas, teclas de función ...).

2. Antecedentes de la técnica

La figura 1 presenta un ejemplo de teclado numérico que comprende una matriz de teclas conectada a un procesador 10. En este ejemplo, la matriz de teclas comprende diez teclas (asociadas a los números del 0 al 9), cuatro filas (referenciadas con LG0 a LG3 (LiGne, en inglés) y tres columnas (referenciadas con COL0 a COL2). Cada tecla permite, cuando se pulsa, cortocircuitar una fila y una columna de la matriz. Por ejemplo, la tecla asociada al número 6 hace posible, cuando se pulsa, cortocircuitar la fila LG1 y la columna COL1.

La técnica convencional de gestión de una matriz de teclas consiste, para el procesador 10, en realizar varias iteraciones sucesivas de una fase de escaneo. Tal como se ilustra en la figura 2, cada iteración de la fase de escaneo comprende las etapas siguientes, para cada una de las filas LG0 a LG3 procesadas sucesivamente:

- escritura de un valor lógico predeterminado (nivel lógico “0” en el ejemplo de la figura 2) en la fila; y

- para cada columna COL0 a COL2, lectura (simbolizada por la letra “r” en la figura 2) de un valor lógico en la columna, para determinar si la columna está en cortocircuito con la fila, por comparación entre el valor lógico leído y el valor lógico predeterminado.

En otras palabras, cuando ejecuta una iteración de la fase de escaneo, el procesador escribe en las filas una por una y lee en las columnas simultáneamente. De este modo, el procesador puede detectar que se ha pulsado una sola tecla, o que se han pulsado varias teclas simultáneamente.

En el ejemplo de la figura 2 y a partir de la descripción, la escritura en las filas y la lectura en las columnas se realizan en un nivel lógico “0”, suponiendo que las filas y columnas están, por defecto, en el valor lógico “1”. Está claro, no obstante, que el principio sigue siendo el mismo si se invierte la utilización de los niveles lógicos “0” y “1” (es decir, si la escritura en las filas y la lectura en las columnas se realizan en el nivel lógico “1”, suponiendo que las filas y columnas están, por defecto, en el valor lógico “0”).

Se considera que la formulación anterior, que se basa en una matriz de teclas (matriz M) y las nociones de escrituras sucesivas en las filas de esta matriz M y de lecturas simultáneas en las columnas de esta matriz M son genéricas. De hecho, existe una alternativa que consiste en escribir sucesivamente en las columnas de esta matriz M y en leer simultáneamente en las filas de esta matriz M. Pero esta alternativa puede ser procesada según la formulación anterior, si consideramos una nueva matriz M en la que las filas corresponden a las columnas de la matriz M y las columnas corresponden a las filas de la matriz M.

En el ejemplo de la figura 2, se supone que se ha pulsado la tecla 6. Por lo tanto, el procesador detecta un cortocircuito entre la fila LG1 y la columna COL1, y deduce que la tecla 6 situada en la intersección entre la fila LG1 y la columna COL1 ha sido pulsada.

Existe una necesidad de hacer que la técnica clásica de gestión de una matriz de teclas (es decir, la rutina convencional de escaneo del teclado) sea segura.

Esta problemática se evoca en el documento de patente FR2599525, que indica que existe el riesgo de que personas malintencionadas intenten interceptar un código confidencial en el momento en que pasa del teclado a medios adecuados para el análisis matricial del teclado, por fila y columna. A partir de la descripción, estos medios también se denominan dispositivo de gestión de la matriz de teclas, o incluso, procesador. El documento FR2599525 especifica que el conocimiento de la forma de onda de las señales de análisis del teclado permite a un dispositivo

espía rastrear inmediatamente cualquier información confidencial pulsada en el teclado. Para espiar el teclado, es suficiente tener algunas conexiones (a través de sondas) en las filas y columnas de la matriz de teclas del teclado. El espionaje de las señales presentes en las filas y las columnas de la matriz también se puede llevar a cabo mediante el análisis de las radiaciones electromagnéticas (o EMA, “ElectroMagnetic Analysis, en inglés”). Por el contrario, se supone que las señales que circulan en el interior del dispositivo de gestión de la matriz de teclas son relativamente complejas, lo que dificulta su utilización para recuperar la información confidencial pulsada en el teclado. Por ello, el dispositivo de gestión de la matriz de teclas se denomina “módulo protegido” en el documento FR2599525.

Con el fin de mejorar la seguridad del teclado, el documento FR2599525 propone una implementación, mediante el dispositivo de gestión de la matriz de teclas (“Módulo protegido”), contramedidas dirigidas a obstaculizar la posibilidad de interceptar cualquier información confidencial pulsada en el teclado (código confidencial, por ejemplo) mediante el espionaje del estado de las filas y columnas de la matriz de teclas del teclado.

De manera más precisa, la técnica descrita en el documento FR2599525 combina:

- un primer mecanismo de simulación: el módulo protegido está provisto de enlaces bidireccionales a algunas, al menos, de las columnas y filas del teclado, y el módulo protegido incluye medios para simular falsos accionamientos de teclas, siendo aplicados al menos algunos de los impulsos de interrogación al mismo tiempo al menos a una fila y al menos a una columna;

- un mecanismo de exploración real del teclado: el módulo protegido explora el teclado tecla a tecla, examinando cada vez una fila o columna llamada “analizada de manera efectiva”, que no recibe el impulso de interrogación (procedente del módulo protegido). Durante esta exploración real, se propone asimismo una simulación complementaria cuando el módulo protegido se encuentra en presencia de una no transferencia del comienzo del impulso de interrogación en la columna o fila analizada (es decir, no accionamiento de una o más teclas exploradas): el módulo protegido responde a esta condición aplicando a la columna o fila analizada un impulso ficticio que termina con el impulso de interrogación (su inicio se retrasa, por el contrario, ligeramente, con respecto al inicio del impulso de interrogación, teniendo en cuenta el tiempo de decisión necesario para el módulo protegido);

- un segundo mecanismo de simulación: el módulo protegido no realiza ninguna interrogación real de una tecla seleccionada, durante un tiempo predeterminado correspondiente al tiempo normal de accionamiento de una tecla, genera al mismo tiempo una respuesta falsa atribuible a esta tecla seleccionada.

Se proponen dos realizaciones de estos mecanismos.

En el primer modo de realización, el módulo protegido está provisto de enlaces bidireccionales a todas las columnas del teclado:

- para el primer mecanismo de simulación, el módulo protegido posee un estado de simulación puro, en el que aplica el impulso de interrogación a una fila y a todas las columnas del teclado;

- para el mecanismo de exploración real del teclado (tecla a tecla), el módulo protegido aplica el impulso de interrogación a una fila y a todas las columnas excepto una columna analizada, estando definida la tecla explorada de manera efectiva por la fila interrogada y la columna analizada.

En el segundo modo de realización, el módulo protegido cuenta con enlaces bidireccionales a todas las filas y todas las columnas del teclado:

- para el primer mecanismo de simulación, el módulo protegido posee un estado de simulación pura, en el que aplica el impulso de interrogación a todas las filas y todas las columnas del teclado;

- para el mecanismo de exploración real del teclado (tecla a tecla), el módulo protegido aplica el impulso de interrogación a todas las filas y columnas, excepto a una fila analizada, por otro lado, a todas las filas y columnas excepto a una columna analizada, estando definida la tecla explorada de manera efectiva por la fila y la columna analizadas.

Si bien permite mejorar la seguridad del teclado, la técnica del documento FR2599525 no es óptima. De hecho, la duración y los recursos informáticos necesarios para la ejecución del mecanismo de exploración real del teclado no están optimizados, puesto que se trata de una exploración tecla a tecla.

Se observará que el segundo modo de realización es incluso más costosa en tiempo y en recursos informáticos que el primer modo de realización, puesto que la exploración de cada tecla se realiza en dos tiempos, primero por la fila a la que pertenece la tecla explorada, a continuación, por la columna a la que pertenece esta misma tecla explorada. Por consiguiente, es preciso generar más secuencias de señales de interrogación en un mismo intervalo de tiempo, para no perder información acerca del estado real del teclado.

3. Objetivos de la invención

La invención, en al menos un modo de realización, tiene por objetivo, en particular, superar estos diferentes inconvenientes del estado de la técnica.

De manera más precisa, en al menos un modo de realización de la invención, un objetivo es proporcionar una técnica de gestión segura, mediante un dispositivo (por ejemplo, un procesador), de una matriz de teclas de un teclado.

Al menos un modo de realización de la invención tiene asimismo como objetivo proporcionar una técnica de este tipo que permita una exploración del teclado más rápida que la técnica conocida del documento FR2599525 explicada anteriormente.

Al menos un modo de realización de la invención tiene asimismo como objetivo proporcionar una técnica tal que permita una exploración del teclado que requiere menos recursos informáticos que la técnica conocida a partir del documento FR2599525 explicada anteriormente.

Otro objetivo de al menos un modo de realización de la invención es proporcionar una técnica tal que sea fácil de implementar y poco costosa.

Otro objetivo de la invención es complicar el análisis de las señales por parte de un atacante.

Otro objetivo de la invención es reducir la frecuencia de aparición de la señal residual que permite encontrar la tecla real pulsada (reducción en la aparición y la desaparición de la tecla pulsada).

4. Resumen de la invención

La invención está definida por las reivindicaciones independientes 1, 7, 8 y 9. Las realizaciones están definidas por las reivindicaciones dependientes 2 a 6. En un modo de realización particular de la invención, se propone un procedimiento de gestión, mediante un dispositivo, una matriz de teclas que comprende al menos una fila y al menos dos columnas, permitiendo cada tecla, cuando se pulsa, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el procedimiento al menos una iteración de una fase de escaneo que comprende las etapas siguientes para cada una de las filas procesadas sucesivamente: escritura de un valor lógico predeterminado en la fila; y, para cada columna, lectura de un valor lógico en la columna para determinar si la columna está cortocircuitada con la fila, por comparación entre el valor lógico leído y el valor lógico predeterminado. Para cada una de las filas procesadas sucesivamente:

- la etapa de escritura del valor lógico predeterminado en la fila se realiza durante un intervalo de tiempo predeterminado;

- para cada columna, la etapa de lectura de un valor lógico en la columna se realiza durante una primera parte del intervalo de tiempo predeterminado;

- la fase de escaneo comprende una etapa adicional, para cada columna, de escritura del valor lógico predeterminado en la columna, durante una segunda parte del intervalo de tiempo predeterminado, siendo la duración del intervalo de tiempo predeterminado igual a la suma de las duraciones de las primera y segunda partes.

En otras palabras, durante dicho intervalo de tiempo predeterminado (T), para cada una de dichas columnas:

* la etapa de leer un valor lógico en la columna se lleva a cabo durante una primera parte (T1) de dicho intervalo de tiempo predeterminado (T);

* la fase de escaneo comprende una etapa adicional de escritura del valor lógico predeterminado en la columna, durante una segunda parte (T2) de dicho intervalo de tiempo predeterminado (T), siendo la duración de dicho intervalo de tiempo predeterminado (T) igual a la suma de las duraciones de las primera y segunda partes.

De este modo, el dispositivo (que gestiona la matriz de teclas del teclado) implementa una primera contramedida destinada a hacer que las señales presentes en las columnas sean lo más independientes posible de la tecla o las teclas pulsadas, al tiempo que se reduce la duración de la exploración del teclado. Para ello, para una fila dada en la que escribe durante un intervalo de tiempo T, el dispositivo lee y escribe en cada columna: lectura durante T1 y escritura durante T2, siendo: T1 + T2 = T. Por consiguiente, contrariamente a la técnica conocida a partir del documento FR2599525 (que propone un escaneo tecla a tecla), el dispositivo de la invención escanea simultáneamente todas las teclas asociadas a una misma fila.

Por lo tanto, si se pulsa una tecla asociada a una fila, solo la señal presente en la columna asociada a esta tecla es ligeramente diferente de las señales presentes en las otras columnas. Esta señal no tiene el mismo valor que las otras durante T1, puesto que toma el valor lógico predeterminado en la fila dada. En cambio, es idéntico a las otras señales durante T2, puesto que se escribe el valor lógico predeterminado en todas las columnas. En otras palabras, dentro de un intervalo de tiempo T:

- si no se pulsa ninguna tecla, los bordes que indican el paso al valor lógico predeterminado (comienzo de T2) son síncronos para todas las columnas;

- si se pulsa una tecla, los bordes que indican el paso al valor lógico predeterminado (comienzo de T2) son síncronos para todas las columnas, excepto la columna asociada a la tecla pulsada (para esta columna, este frente corresponde al comienzo de T1, y por lo tanto está anticipado con respecto a los bordes síncronos de las otras columnas).

Se considera que la formulación anterior, que se basa en una matriz de teclas (matriz M) y las nociones de escrituras sucesivas (durante T) en cada una de las filas de esta matriz M y de lecturas (durante T1) y escrituras (durante T2) en cada columna de esta matriz M, es genérica. De hecho, hay una alternativa que consiste en escribir sucesivamente (durante T) en cada una de las columnas de esta matriz M, y leer (durante T1) y escribir (durante T2) en cada una de las filas de la matriz M. Pero esta alternativa puede ser procesada según la formulación anterior, si se considera una nueva matriz M', en la que las filas corresponden a las columnas de la matriz M y las columnas corresponden a las filas de la matriz M.

Según un aspecto particular de la invención, para cada columna, el orden de las etapas de lectura y escritura durante el intervalo de tiempo predeterminado se selecciona de manera aleatoria.

En otras palabras, para cada columna, el dispositivo elige de manera aleatoria entre: una lectura durante T1 y, a continuación, una escritura durante T2, o una escritura durante T2 y, a continuación, una lectura durante T1.

De este modo, el dispositivo (que gestiona la matriz de teclas del teclado) implementa, en combinación con la primera contramedida, una segunda contramedida dirigida a dificultar la detección de una tecla pulsada. El aspecto aleatorio permite asimismo evitar cualquier aprendizaje por parte de un dispositivo espía. De hecho, dentro de un intervalo de tiempo T:

- si no se pulsa ninguna tecla, los bordes que indican la transición al valor lógico predeterminado (comienzo de T2) no son síncronos para todas las columnas, debido a que el orden entre la lectura y la escritura (es decir, entre T1 y T2) no es el mismo para todas las columnas,

- si se pulsa una tecla, los bordes que indican la transición al valor lógico predeterminado (comienzo de T2) tampoco son síncronos para todas las columnas (para la columna asociada a la tecla pulsada, este borde no es fácil de localizar mediante una simple comparación con los bordes síncronos de las otras columnas).

Ventajosamente, en cada intervalo de tiempo predeterminado, la duración de la segunda parte del intervalo de tiempo predeterminado es idéntica para todas las columnas.

De esta manera, se incrementa el parecido entre las señales presentes en las diferentes columnas, y se dificulta aún más la detección de una tecla pulsada.

Según una característica particular, la matriz de teclas comprende una pluralidad de filas, y se caracteriza por que, en cada iteración de la fase de escaneo, el orden de procesamiento sucesivo de las filas es aleatorio.

Por lo tanto, el dispositivo (que gestiona la matriz de teclas del teclado) implementa una tercera contramedida para aumentar aún más la complejidad del análisis de las señales presentes en las filas y las columnas, que debe realizar un dispositivo espía para determinar cualquier información confidencial que se introduzca en las teclas del teclado.

Según un aspecto particular de la invención, la matriz de teclas comprende una pluralidad de filas, y se caracteriza por que, durante una iteración dada de la fase de escaneo, al menos un parámetro varía de manera aleatoria, de una fila a otra, perteneciendo dicho al menos un parámetro al grupo que comprende:

- la duración del intervalo de tiempo predeterminado;

- la duración de la primera parte del intervalo de tiempo predeterminado; y

- la duración de la segunda parte del intervalo de tiempo predeterminado.

Por lo tanto, el dispositivo (que gestiona la matriz de teclas del teclado) implementa una cuarta contramedida que permite aumentar aún más la complejidad del análisis de las señales presentes en las líneas y las columnas.

Según una característica particular, al menos una iteración de la fase de escaneo, que sigue a una iteración durante la cual se ha determinado un cortocircuito entre una columna dada y una fila dada, comprende las etapas siguientes:

- para cada una de las filas procesadas sucesivamente, distintas de una fila dada en cortocircuito con una columna dada:

  * para cada columna, escritura del valor lógico predeterminado en la columna durante el intervalo de tiempo;

- para cada fila dada en cortocircuito con una columna dada:

  * para cada columna distinta de la columna dada, escritura del valor lógico predeterminado en la columna durante toda la duración del intervalo de tiempo; y

  * para la columna dada, lectura de un valor lógico durante la primera parte del intervalo de tiempo, a fin de detectar una continuación o una detención de dicho cortocircuito entre la columna dada y la fila dada, y escritura del valor lógico predeterminado durante la segunda parte del intervalo de tiempo.

Por lo tanto, el dispositivo (que gestiona la matriz de teclas del teclado) implementa una quinta contramedida que permite ocultar una pulsación sobre una tecla o sobre varias teclas. De hecho, tan pronto como se detecta una pulsación de una tecla durante una iteración de la fase de escaneo, el comportamiento del dispositivo en las iteraciones siguientes de la fase de escaneo es tal que, mientras se pulsa esta tecla, las señales presentes en todas las columnas son idénticas (valor lógico predefinido durante T). Por lo tanto, solo durante dos iteraciones (la de detección de la tecla pulsada y la de detección de la liberación de la tecla) puede saber un dispositivo espía qué tecla ha sido pulsada. En contrapartida, una pulsación sobre otra tecla no puede ser detectada hasta la iteración de detección de la liberación de la tecla pulsada. Es asimismo posible gestionar teclas simultáneas si aparecen al mismo tiempo en una misma y única fase de detección, lo que es extremadamente poco probable en la práctica.

En otro modo de realización de la invención, se ha propuesto un programa informático que comprende instrucciones de código de programa para implementar el procedimiento citado anteriormente (en uno cualquiera de sus diversas realizaciones), cuando dicho programa es ejecutado en un ordenador o un procesador.

En otro modo de realización de la invención, se propone un medio de almacenamiento legible por ordenador y no transitorio, que se almacena un programa informático que comprende un conjunto de instrucciones ejecutables por un ordenador o un procesador para implementar el procedimiento citado anteriormente (en cualquiera de sus diferentes realizaciones).

En otro modo de realización de la invención, se propone un dispositivo de gestión de una matriz de teclas que comprende al menos una fila y al menos dos columnas, permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el dispositivo medios de escaneo adaptados para realizar al menos una iteración de una fase de escaneo, comprendiendo los medios de escaneo los medios siguientes, activados para cada una de las filas procesadas sucesivamente: medios de escritura de un valor lógico predeterminado en la fila; y medios de lectura de un valor lógico en cada columna para determinar si la columna está cortocircuitada con la fila, por comparación entre el valor lógico leído y el valor lógico predeterminado. Para cada una de las filas procesadas sucesivamente: los medios para escribir el valor lógico predeterminado en la fila son activados durante un período de tiempo predeterminado; para cada columna, los medios para leer un valor lógico en la columna son activados durante una primera parte del intervalo de tiempo predeterminado. Los medios de escaneo comprenden medios de escritura adicionales, activados para cada columna durante una segunda parte del intervalo de tiempo predeterminado para escribir el valor lógico predeterminado en la columna, siendo la duración del intervalo de tiempo predeterminado igual a la suma de las duraciones de las primera y segunda partes.

En otras palabras, los medios de escaneo comprenden medios adicionales de escritura, y para cada fila procesada sucesivamente:

- los medios de escritura del valor lógico predeterminado en la fila son activados durante un intervalo de tiempo predeterminado (T);

- durante dicho intervalo de tiempo predeterminado (T), para cada una de dichas columnas:

  * los medios de lectura de un valor lógico en la columna son activados durante una primera parte (T1) de dicho intervalo de tiempo predeterminado (T);

  * los medios de escritura adicionales son activados durante una segunda parte (T2) de dicho intervalo de tiempo predeterminado (T), para escribir el valor lógico predeterminado en la columna, siendo la duración del intervalo de tiempo predeterminado igual a la suma de las duraciones de las primera y segunda partes.

Ventajosamente, el dispositivo de gestión de la matriz de teclas comprende medios para implementar etapas que realiza en el procedimiento descrito anteriormente, en cualquiera de sus diferentes realizaciones.

5. Lista de las figuras

Otras características y ventajas de la invención resultarán evidentes con la lectura de la siguiente descripción, dada a título de ejemplo indicativo y no limitativo, y de los dibujos que se acompañan, en los cuales:

- la figura 1, ya descrita en relación con la técnica anterior, presenta un ejemplo de un teclado numérico que comprende una matriz de teclas ligada a un procesador;

- la figura 2, ya descrita en relación con la técnica anterior, ilustra la técnica convencional de gestión de la matriz de teclas de la figura 1, en el caso en el que se pulsa la tecla 6;

- la figura 3 ilustra una primera contramedida, según un modo de realización particular de la invención, si se pulsa la tecla 6;

- las figuras 4, 5 y 6 ilustran una combinación de la primera contramedida con una segunda contramedida, según un modo de realización particular de la invención (ninguna tecla pulsada en la figura 4; tecla 6 pulsada y detectada en el intervalo de tiempo A, en la figura 5, y en el intervalo de tiempo C, en la figura 6);

- la figura 7 ilustra una tercera contramedida, que puede ser combinada con la primera (y con una cualquiera de las otras contramedidas);

- la figura 8 ilustra una combinación de las primera y segunda contramedidas con una cuarta contramedida, según un modo de realización particular de la invención (ninguna tecla pulsada);

- las figuras 9, 10 y 11 ilustran una combinación de las primera y segunda contramedidas con una quinta contramedida, según un modo de realización particular de la invención (primera detección de la tecla 6 pulsada, en la figura 9; confirmación de la detección de la tecla 6 pulsada, en la figura 10); detección de la tecla 6 liberada, en la figura 11); y

- la figura 12 presenta la estructura de un dispositivo de gestión de una matriz de teclas de un teclado, según un modo de realización particular de la invención.

6. Descripción detallada

Con la intención de simplificar, se utiliza a partir de la descripción, el ejemplo de teclado de la figura 1, con una matriz de teclas que comprende diez teclas (asociadas a los números 0 a 9), cuatro filas (referenciadas con LG0 a LG3) y tres columnas (referenciadas con COL0 a COL2). Es claro que las contramedidas que se presentan a continuación, según diferentes realizaciones de la invención, no se limitan a este ejemplo de un teclado.

Cada una de las figuras 3 a 6 y 8 a 11 presenta los valores lógicos presentados en las filas LG0 a LG3 y las columnas COL0 a COL2, durante una iteración de la fase de escaneo. La figura 7 presenta los valores lógicos presentes en las filas LG0 a LG3, durante dos iteraciones de la fase de escaneo.

Se supone que los impulsos de interrogación poseen un nivel lógico “0”. No obstante, está claro que el principio sigue siendo el mismo si se invierte la utilización de los niveles lógicos “0” y “1”.

A continuación, se presenta, en relación con la figura 3, una primera contramedida, según un modo de realización particular de la invención. Se supone que se pulsa la tecla 6.

Durante el intervalo de tiempo T de escritura de un impulso de interrogación (nivel lógico “0”) en cada una de las filas LG0 a LG3, el procesador realiza las siguientes etapas para cada columna COL0 a COL2:

- lectura (simbolizada por la letra “r” en la figura 3) de un valor lógico en la columna durante una primera parte T1 del intervalo de tiempo T, para determinar si la columna está en cortocircuito con la fila (por comparación entre el valor lógico leído y el valor lógico “0”);

- escritura (simbolizada por la letra “w” en la figura 3) del valor lógico “0” en la columna durante una segunda parte T2 del intervalo de tiempo T (siendo la duración de T igual a la suma de las duraciones de T1 y T2).

Por lo tanto, en la iteración de la fase de escaneo presentada en la figura 3, cada una de las filas LG0 a LG3 puede adoptar uno de los estados siguientes:

- fuera del intervalo de tiempo T, un estado “no forzado por el procesador”, en el que la fila adopta:
  - el valor lógico “1” por defecto, si esta fila no está cortocircuitada con una columna; o
  - el valor lógico de una columna dada, si esta fila está cortocircuitada con esta columna dada (es decir, si se pulsa la tecla asociada a esta fila y esta columna);
- durante el intervalo de tiempo T, un estado “forzado por el procesador”, en el que la fila adopta el valor lógico “0” escrito por el procesador.

De manera similar, en la iteración de la fase de escaneo presentada en la figura 3, cada una de las columnas COL0 a COL2 puede adoptar uno de los estados siguientes:

- fuera del intervalo de tiempo T, un estado “no forzado por el procesador”, en el que la columna adopta el valor lógico “1” por defecto;

- durante la primera parte T1 del intervalo de tiempo T, un estado “no forzado por el procesador” (el procesador lee esta columna), en el que la columna adopta:

  - el valor lógico “1” por defecto, si esta columna ya no está en cortocircuito con una línea en la que el procesador ha escrito el valor “0”; o

  - el valor lógico “0”, si esta columna está en cortocircuito con una línea en la que el procesador ha escrito el valor “0”.

- durante la segunda parte T2 del intervalo de tiempo T, un estado “forzado por el procesador”, en el que la columna adopta el valor lógico “0” escrito por el procesador.

En el ejemplo de la figura 3, la tecla 6 (asociada a la fila LG1 y la columna COL1) está pulsada. Por consiguiente, para cada una de las columnas COL0 y COL2, el procesador lee el valor lógico “1” durante cada primera parte T1 del intervalo de tiempo T, y escribe el valor “0” durante cada segunda parte T2 del intervalo de tiempo T. Para la columna COL1, el procesador también actúa, con la excepción del intervalo de tiempo T de escritura en la fila LG1, durante el cual el procesador lee el valor lógico “0” durante la primera parte T1 de este intervalo de tiempo (puesto que la fila LG1 está cortocircuitada con la columna COL1) y escribe el valor “0” durante la segunda parte T2 de este intervalo de tiempo. Se debe observar que, por el hecho de pulsar la tecla 6, el valor de la fila LG1 sigue al de la columna COL1.

Un estado “no forzado”, para una fila o columna, corresponde a un puerto del procesador conectado a esta fila o columna y configurado como entrada, con una resistencia de accionamiento a un estado alto (“resistencia pull-up”, en inglés) o bajo (“resistencia pull-down”, en inglés), fijando esta resistencia de accionamiento el nivel eléctrico.

Un estado “forzado”, para una fila o columna, corresponde a un puerto del procesador conectado a esta fila o columna y configurado en la salida, a un nivel lógico “1” o “0”.

La primera contramedida presentada anteriormente es vulnerable a un análisis detallado de las señales presentes en las columnas COL0 a COL2, puesto que se puede observar que para el par (LG1, COL1), los bordes descendentes son síncronos, mientras que para los demás pares (fila, columna) el borde descendente de la señal de columna está desfasado (en T1) con respecto al borde descendente de la señal de fila.

A continuación, se presenta, en relación con las figuras 4, 5 y 6, una combinación de la primera contramedida con una segunda contramedida, según un modo de realización particular de la invención.

Para superar la debilidad de la primera contramedida, esta es combinada con la segunda contramedida que consiste, para el procesador 10, en seleccionar de manera aleatoria el orden de las operaciones de lectura (durante T1) y de escritura (durante T2), para cada columna COL0 a COL2.

Además, durante cada intervalo de tiempo T, la duración de T2 (escritura por parte del procesador) es idéntica para todas las columnas.

En las figuras 4, 5 y 6, cada intervalo de tiempo T (escritura de un impulso de interrogación en una fila) está dividido en tres porciones llamadas A, B y C, respectivamente. Para cada columna COL0 a COL2, se cumple: T1 = A y T2 = B + C (es decir, lectura en A y escritura en B y C), o bien: T1 = C y T2 = A + B (es decir, lectura en C y escritura en A y B).

En el ejemplo de las figuras 4 y 6, se cumple:

- T1 = A y T2 = B + C, para los pares siguientes: (LG0, COL0), (LG0, COL2), (LG1, COL0), (LG2, COL0), (LG2, COL1), (LG2, COL2) y (LG3, COL1);

- T1 = C y T2 = A + B, para los pares siguientes: (LG0, COL1), (LG1, COL1), (LG1, COL2), (LG3, COL0) y (LG3, COL2).

El ejemplo de la figura 5 se distingue del de las figuras 4 y 6 únicamente para el par (LG1, COL1), para el cual se cumple: T1 = A y T2 = B + C (es decir, lectura en A en lugar de lectura en C).

Se hacen las suposiciones siguientes: en la figura 4 no está pulsada ninguna tecla. En la figura 5, la tecla 6 está pulsada y, por consiguiente, es detectada en la porción A. En la figura 6, la tecla 6 está pulsada y se detecta en la porción C.

A continuación, se presenta, en relación con la figura 7, una tercera contramedida, según un modo de realización particular de la invención. Puede ser combinada con la primera contramedida (sola o en combinación con cualquiera de las otras contramedidas).

Con el fin de aumentar aún más la complejidad del análisis de las señales de las columnas y hacer que el proceso. implementado por el procesador sea aún menos predecible, la tercera contramedida consiste en elegir al azar el

orden en el que el procesador escribe el impulso de interrogación en las filas, en cada iteración de la fase de escaneo.

En el ejemplo de la figura 7, en una primera iteración referenciada con 71, el procesador escribe en las filas en el orden siguiente: LG1, LG0, LG3 y LG2. En otra iteración referenciada con 72, el procesador escribe en las filas en el orden siguiente: LG2, LG1, LG3 y LG0.

A continuación, se presenta, en relación con la figura 8, una combinación de las primera y segunda contramedidas con una cuarta contramedida.

La cuarta contramedida consiste, para el procesador, en variar de manera aleatoria, de una fila a la otra, uno o más de los parámetros siguientes, a cada iteración de la fase de escaneo:

- la duración del intervalo de tiempo predeterminado T;

- la duración de la primera parte T1 (lectura por parte del procesador) del intervalo de tiempo T; y

- la duración de la segunda parte T2 (escritura por parte del procesador) del intervalo de tiempo T.

De este modo, se evita un espionaje con activación en un ancho específico.

En el ejemplo de la figura 8, solo la duración de la porción B varía de manera aleatoria, por lo que la duración del intervalo de tiempo predeterminado T también varía de manera aleatoria (este es asimismo el caso de la duración de la segunda parte T2, puesto que T2 es igual a + B o B + C). En cambio, la duración de la primera parte T1 no es variable en este ejemplo (puesto que T1 es igual a o C).

A continuación, se presenta, en relación con las figuras 9, 10 y 11, una combinación de las primera y segunda contramedidas con una quinta contramedida, según un modo de realización particular de la invención.

La quinta contramedida consiste en, después que se detecta que una tecla ha sido pulsada durante una iteración de la fase de escaneo (denominada a continuación en el presente documento, iteración de detección de pulsación), ocultar esta tecla pulsada durante las iteraciones siguientes de la fase de escaneo (denominadas a continuación en el presente documento iteraciones de confirmación de pulsación), hasta que se detecte una liberación de esta tecla durante una iteración de la fase de escaneo, denominada a continuación en el presente documento iteración de detección de liberación.

La figura 9 presenta un ejemplo de una iteración de detección de pulsación, en la que se detecta una pulsación de la tecla 6 (lectura en A del valor lógico “0” y, a continuación, escritura en B y C del valor lógico “0”, para el par (LG1, COL1)). Esta figura 9 es idéntica a la figura 5 y no se describe de nuevo.

La figura 10 presenta un ejemplo de una iteración de confirmación de pulsación, en la que se confirma la pulsación de la tecla 6 (para el par (LG1, COL1), lectura en A del valor lógico “0” y, a continuación, escritura del valor lógico “0” en B y C, es decir, T1 = A y T2 = B + C). Para ocultar la pulsación de esta tecla 6, para todos los demás pares (fila, columna), el procesador no realiza ninguna lectura en las columnas, sino que escribe únicamente el valor lógico “0” durante toda la duración del intervalo de tiempo T del impulso de interrogación (escritura durante A, B y C, es decir, T2 = A + B + C = T). Por lo tanto, para cada intervalo de tiempo T, todas las señales presentes en las diferentes columnas son estrictamente idénticas (valor lógico “0” durante T).

La figura 11 muestra un ejemplo de una iteración de detección de liberación, en la que se detecta la liberación de la tecla 6 (para el par (LG1, COL1), lectura en A del valor lógico “1” y, a continuación, escritura del valor lógico “0” en B y C, es decir, T1 = A y T2 = B + C).

La figura 12 presenta la estructura de un dispositivo 10 de gestión de una matriz de teclas de un teclado, según un modo de realización particular de la invención. Este dispositivo implementa las contramedidas presentadas anteriormente, o una combinación de algunas de ellas.

En este ejemplo, el dispositivo comprende una memoria de acceso aleatorio RAM 123 (“Random Access Memory” en inglés), una unidad central de procesamiento 121 (o CPU, “Central Processing Unit” en inglés), equipada, por ejemplo, con un procesador y controlado por un programa almacenado en una memoria de solo lectura ROM 122 (“Read Only Memory” en inglés). En la inicialización, las instrucciones de código del programa son cargadas, por ejemplo, en la memoria RAM 123 antes de ser ejecutadas por la unidad de procesamiento 121. La unidad de procesamiento 121 gestiona las señales en las filas y las columnas (LG0 a LG3 y COL0 a COL2 en este ejemplo) de la matriz de teclas del teclado, según las instrucciones de programa 122, para implementar todas o una parte de las contramedidas detalladas anteriormente.

Esta figura 12 ilustra solamente una manera particular, de entre varias posibles, de realizar las diferentes contramedidas detalladas anteriormente, en relación con las figuras 3 a 11. De hecho, la técnica de la invención se realiza indistintamente:

- en una máquina de cálculo reprogramable (un procesador o un microcontrolador, por ejemplo), que ejecuta un programa que comprende una secuencia de instrucciones, o

- en una máquina de cálculo exclusiva (por ejemplo, un conjunto de puertas lógicas tal como una FPGA o un ASIC, o cualquier otro módulo de hardware).

En el caso de que la invención esté implantada en una máquina de cálculo reprogramable, el programa correspondiente (es decir, la secuencia de instrucciones) puede estar almacenado en un medio de almacenamiento extraíble (tal como, por ejemplo, un disquete, un CD-ROM o un DVD-ROM) o no, siendo legible este medio de almacenamiento de manera parcial o completa mediante un ordenador o un procesador.

REIVINDICACIONES

1. Procedimiento de gestión, mediante un dispositivo (10), de una matriz de teclas que comprende al menos una fila (LG0 a LG3) y dos columnas (COL0 a COL2), permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el procedimiento al menos una iteración de una fase de escaneo que comprende las etapas siguientes para cada una de las filas procesadas sucesivamente:

- escritura de un valor lógico predeterminado en la fila; y

- para cada columna, lectura de un valor lógico en la columna para determinar si la columna está cortocircuitada con la fila, por comparación entre el valor lógico leído y el valor lógico predeterminado,

caracterizado por que, para cada una de las filas procesadas sucesivamente:

- la etapa de escritura del valor lógico predeterminado en la fila se efectúa durante un intervalo de tiempo predeterminado (T);

- durante dicho intervalo de tiempo predeterminado (T), una etapa de exploración simultánea de todas las teclas asociadas con la misma fila que comprende, para cada una de dichas columnas:

  * la etapa de lectura de un valor lógico en la columna se realiza durante una primera parte (T1) de dicho intervalo de tiempo predeterminado (T);

  * la fase de escaneo comprende una etapa de escritura adicional del valor lógico predeterminado en la columna, durante una segunda parte (T2) de dicho intervalo de tiempo predeterminado (T), la duración de dicho intervalo de tiempo predeterminado (T) es igual a la suma de las duraciones de las primera y segunda partes.

2. Procedimiento según la reivindicación 1, caracterizado por que, para cada columna, el orden de las etapas de lectura y escritura durante el intervalo de tiempo predeterminado es seleccionado de manera aleatoria.

3. Procedimiento según la reivindicación 2, caracterizado por que, en cada intervalo de tiempo predeterminado, la duración de la segunda parte del intervalo de tiempo predeterminado es idéntica para todas las columnas.

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que la matriz de teclas comprende una pluralidad de filas y por que, en cada iteración de la fase de escaneo (71, 72), el orden de procesamiento sucesivo de las filas es aleatorio.

5. Procedimiento según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que la matriz de teclas comprende una pluralidad de filas, y por que, durante una iteración dada de la fase de escaneo, al menos un parámetro varía de manera aleatoria, de una fila a otra, perteneciendo dicho al menos un parámetro al grupo que comprende:

- la duración del intervalo de tiempo predeterminado;

- la duración de la primera parte del intervalo de tiempo predeterminado; y

- la duración de la segunda parte del intervalo de tiempo predeterminado.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que al menos una iteración de la fase de escaneo, que sigue a una iteración durante la cual se ha determinado al menos un cortocircuito entre una columna dada y una fila dada, comprende las etapas siguientes:

- para cada una de las filas procesadas sucesivamente, excepto una fila dada en cortocircuito con una columna dada:

  * para cada columna, escritura del valor lógico predeterminado en la columna durante toda la duración del intervalo de tiempo;

- para cada fila dada en cortocircuito con una columna dada:

  * para cada columna distinta de la columna dada, escritura del valor lógico predeterminado en la columna durante toda la duración del intervalo de tiempo; y

  * para la columna dada, lectura de un valor lógico durante la primera parte del intervalo de tiempo, para detectar una continuación o una parada de dicho cortocircuito entre la columna dada y la fila dada, y escritura del valor lógico predeterminado durante la segunda parte del intervalo de tiempo.

7. Programa informático, que comprende instrucciones de código de programa para la implementación del procedimiento según una de las reivindicaciones 1 a 6, cuando dicho programa es ejecutado en un ordenador o un procesador.

8. Medio de almacenamiento legible por ordenador y no transitorio, que almacena un programa informático que comprende un conjunto de instrucciones ejecutables por un ordenador o procesador para implementar el procedimiento según una de las reivindicaciones 1 a 6.

9. Dispositivo de gestión de una matriz de teclas que comprende al menos una fila y al menos dos columnas, permitiendo cada tecla, cuando es pulsada, cortocircuitar una fila y una columna de dicha matriz, comprendiendo el dispositivo medios de escaneo adaptados para realizar al mismo tiempo una iteración de una fase de escaneo, comprendiendo los medios de escaneo los siguientes medios, activados para cada fila procesada sucesivamente:

- medios de escritura de un valor lógico predeterminado en la fila; y

- medios de lectura de un valor lógico en cada columna para determinar si la columna está cortocircuitada con la fila, por comparación entre el valor lógico leído y el valor lógico predeterminado,

caracterizado por que los medios de escaneo comprenden medios adicionales de escritura,

y por que, para cada una de las filas procesadas sucesivamente:

- los medios de escritura del valor lógico predeterminado en la fila son activados durante un intervalo de tiempo predeterminado (T);

- durante dicho intervalo de tiempo predeterminado (T), una etapa de exploración simultánea de todas las teclas asociadas a la misma fila es activada y comprende, para cada una de dichas columnas:

  * los medios de lectura de un valor lógico en la columna son activados durante una primera parte (T1) de dicho intervalo de tiempo predeterminado (T);

  * los medios de escritura adicionales son activados durante una segunda parte (T2) de dicho intervalo de tiempo predeterminado (T), para escribir el valor lógico predeterminado en la columna, siendo igual la duración del intervalo de tiempo predeterminado a la suma de las duraciones de las primera y segunda partes.

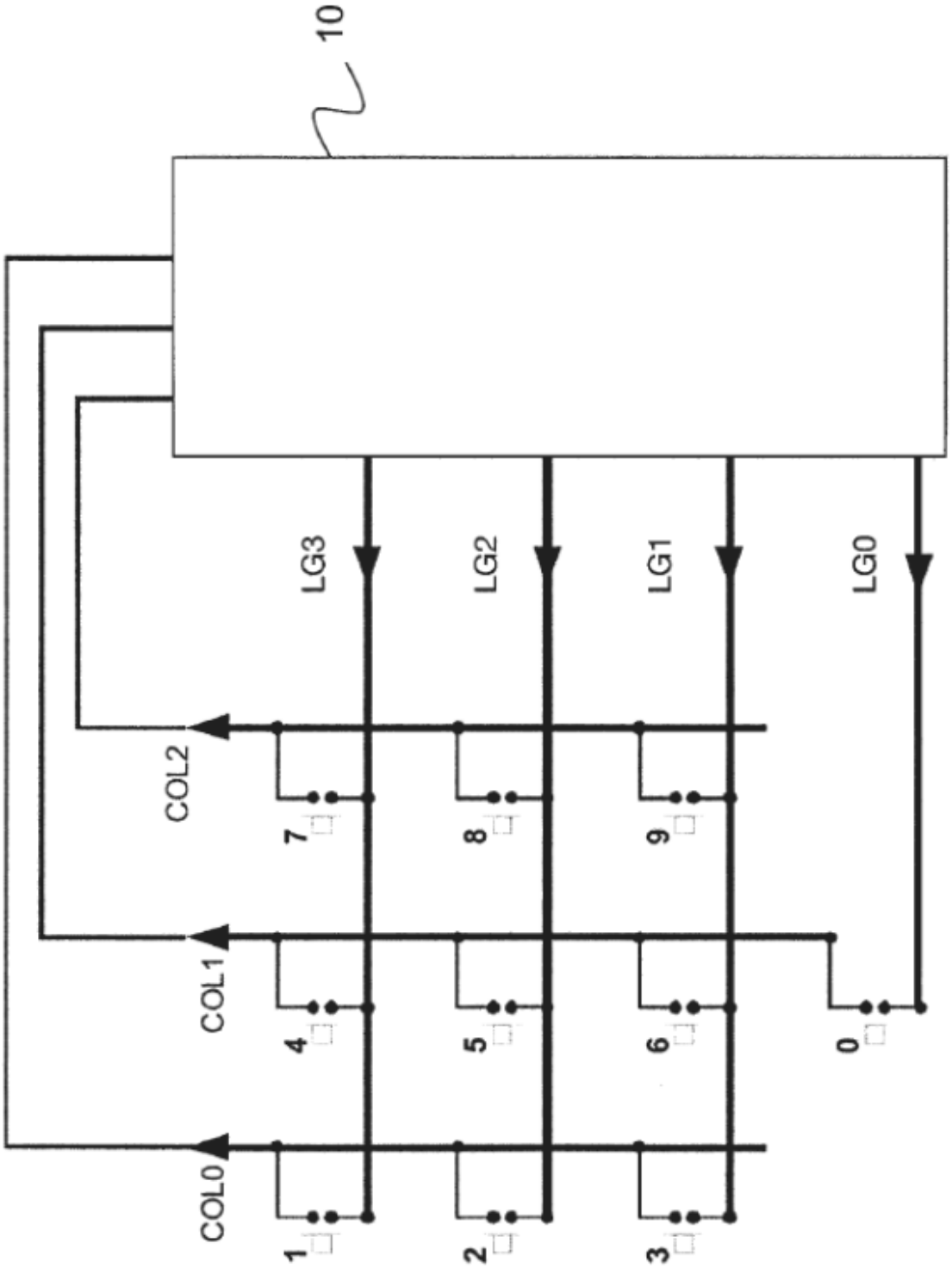

Figura 1

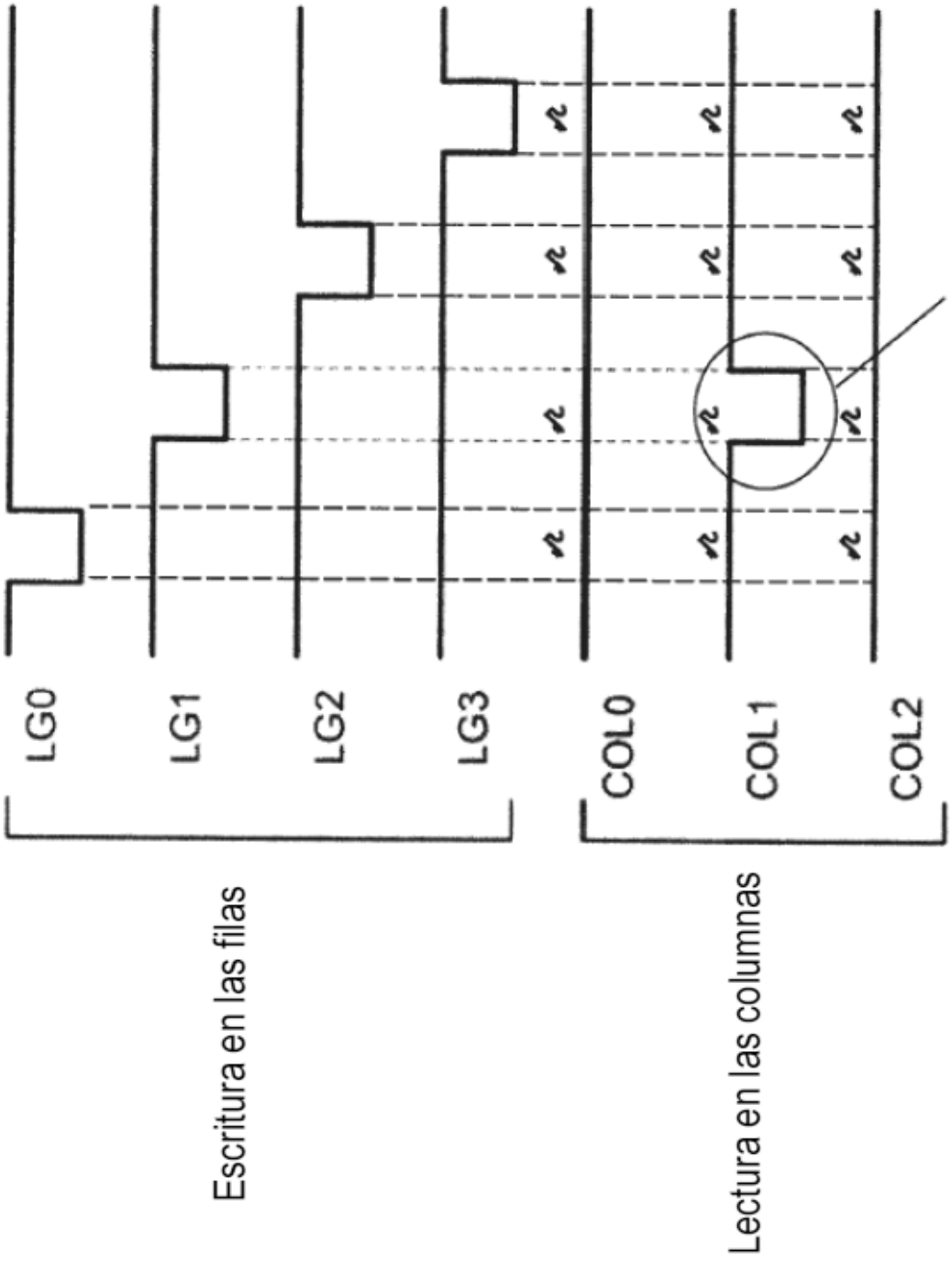
LG0
LG1
LG2
LG3
COL0
COL1
COL2
Escritura en las filas
Lectura en las columnas
Detección de tecla 6 pulsada

Figura 2

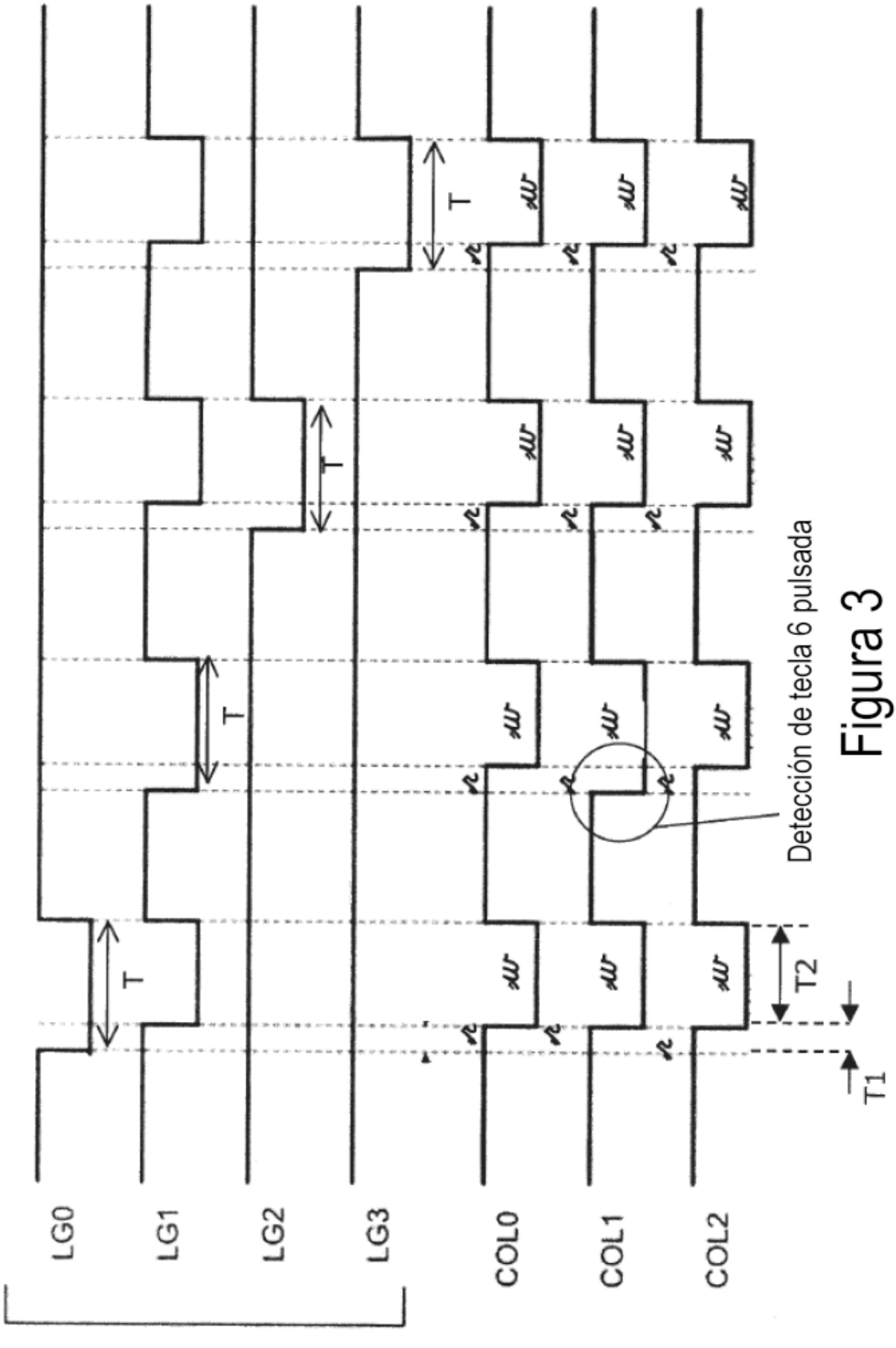
LG0
LG1
LG2
LG3
COL0
COL1
COL2
T
T
T
T
T2
T1
Detección de tecla 6 pulsada

Figura 3

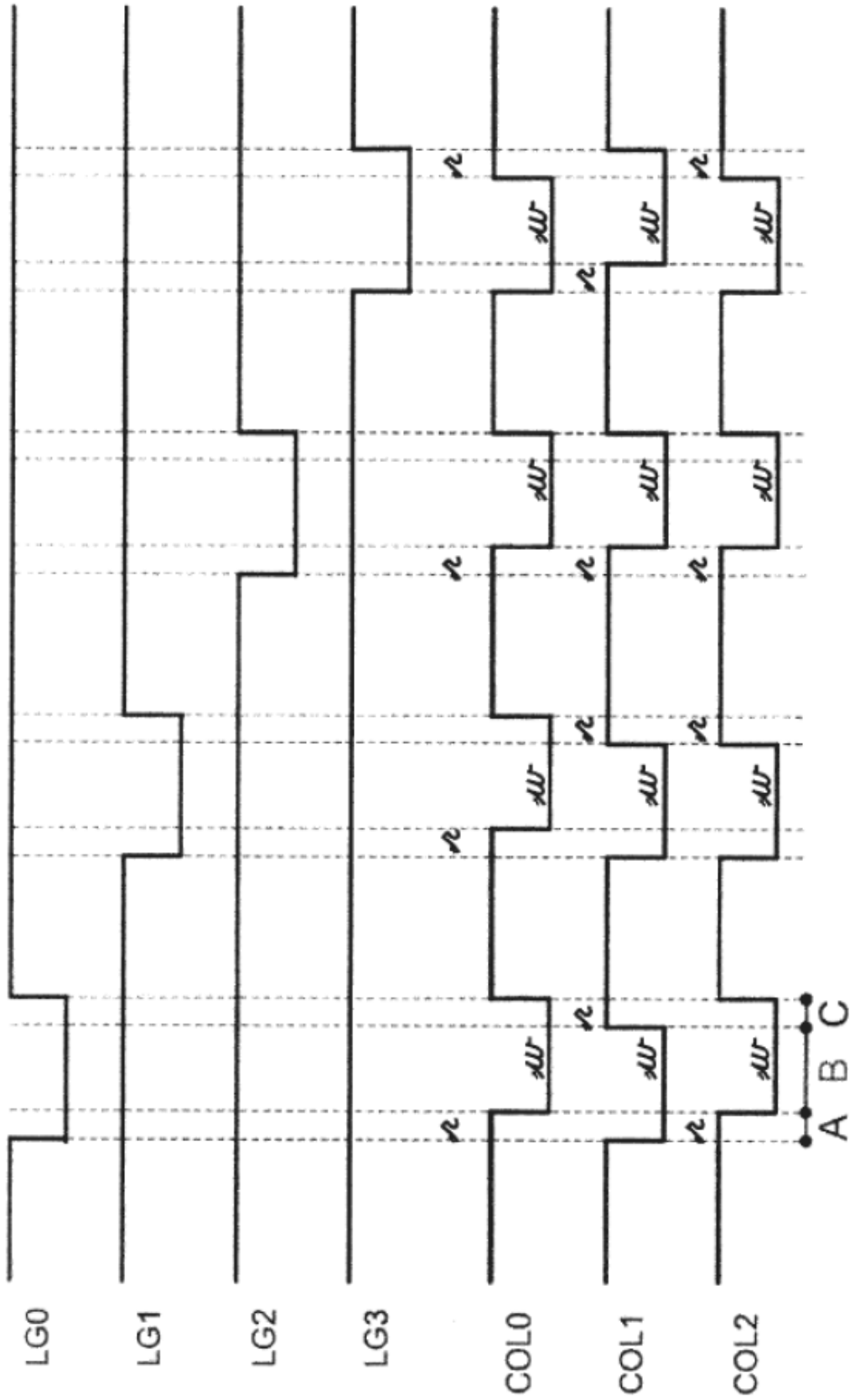

Figura 4

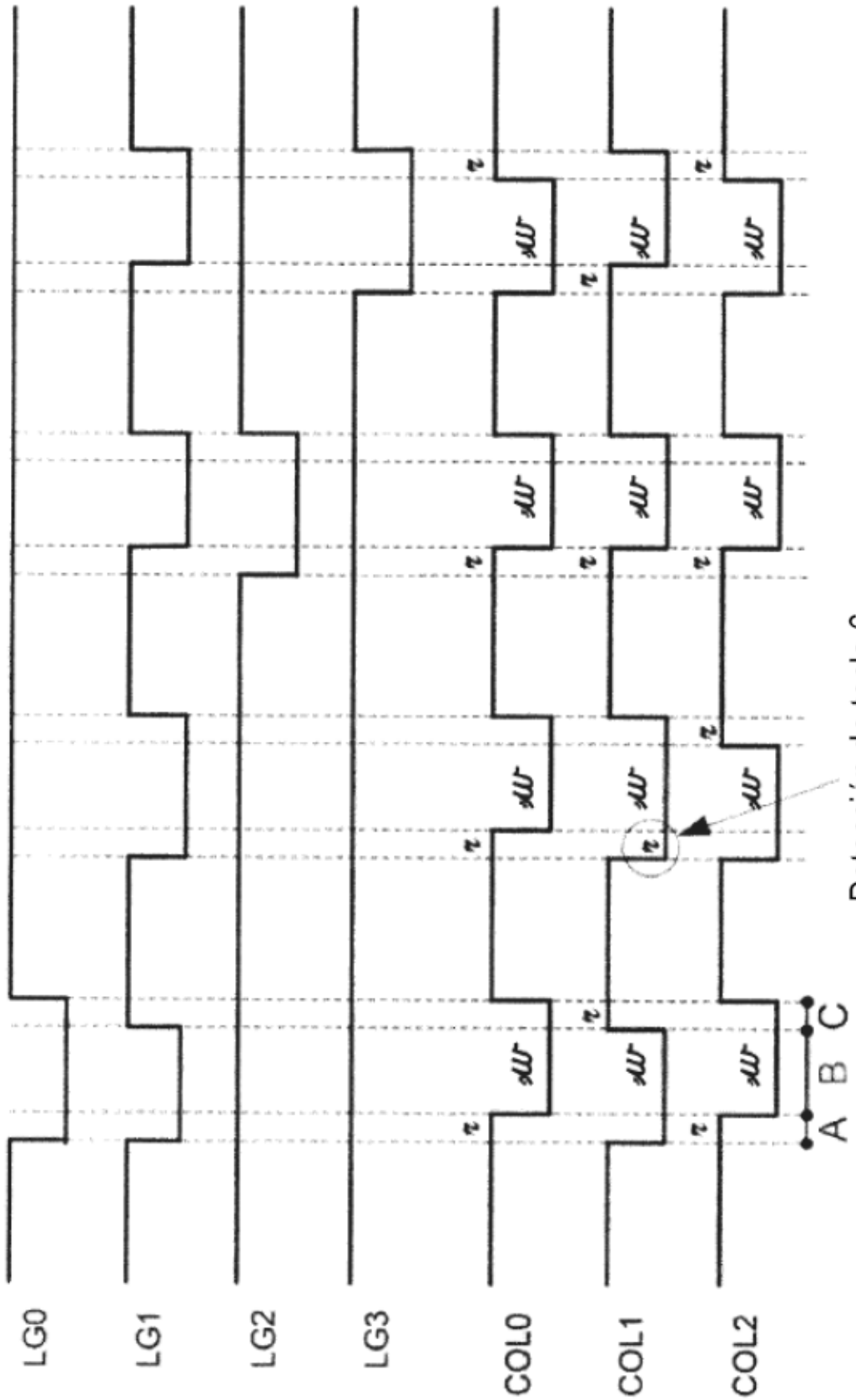
LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Detección de tecla 6
pulsada, lectura en A

Figura 5

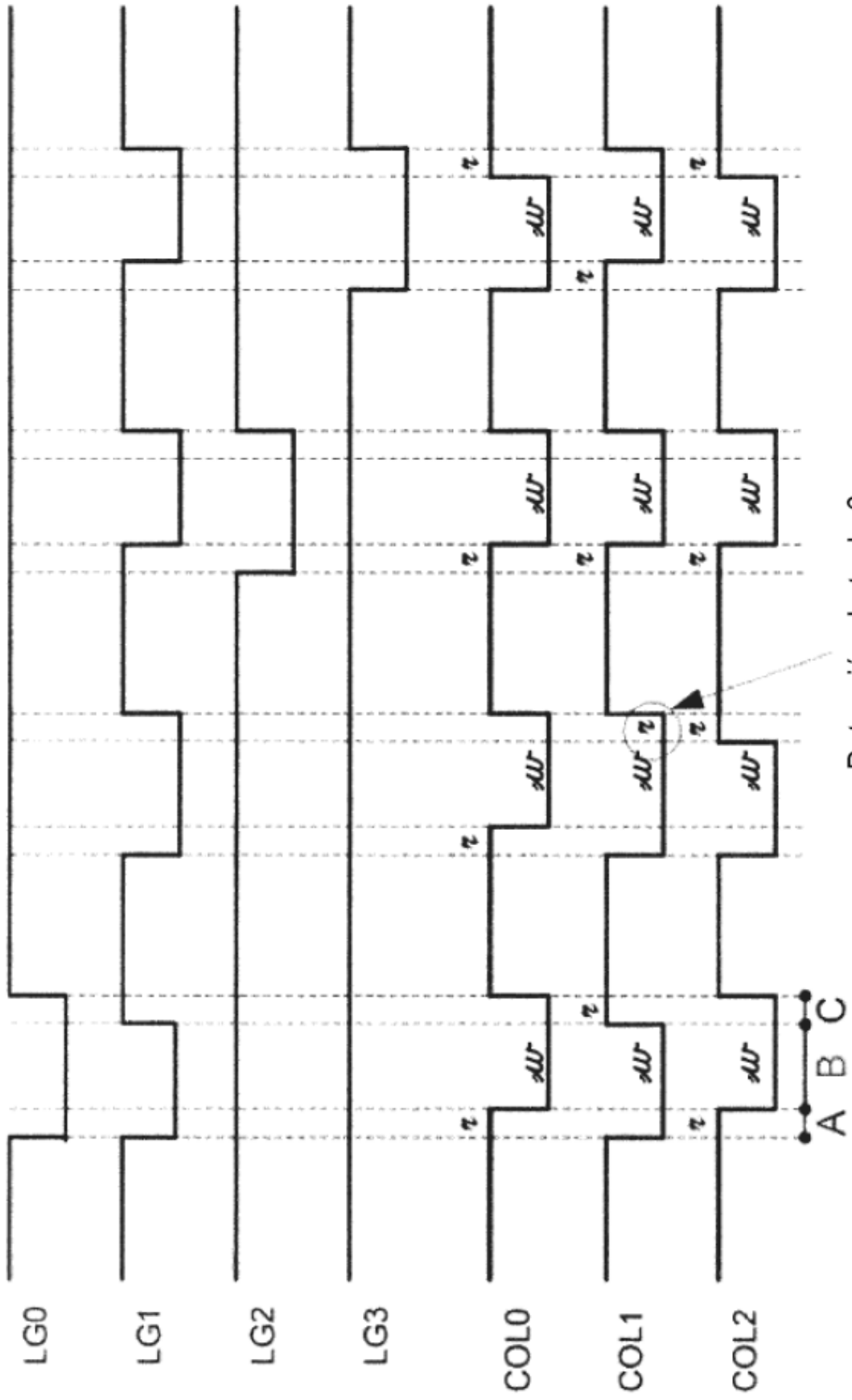
LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Detección de tecla 6
pulsada, lectura en C

Figura 6

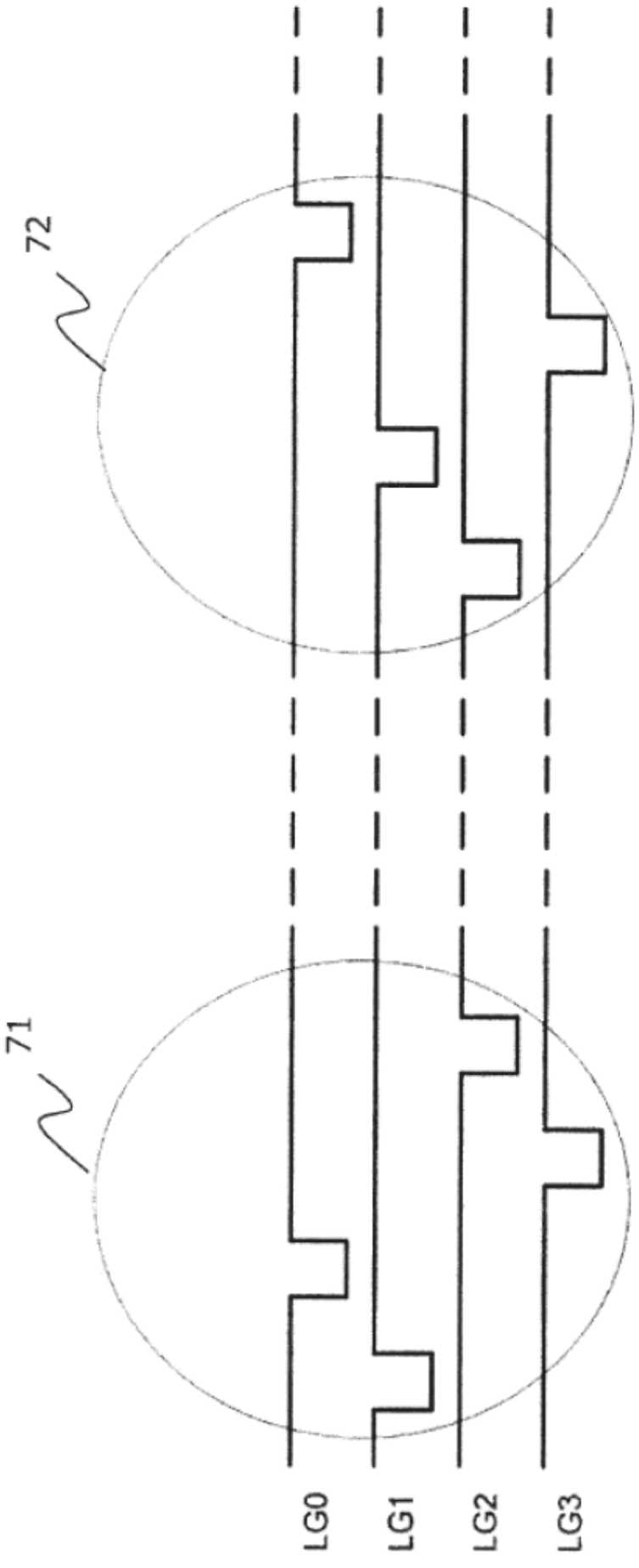

Figura 7

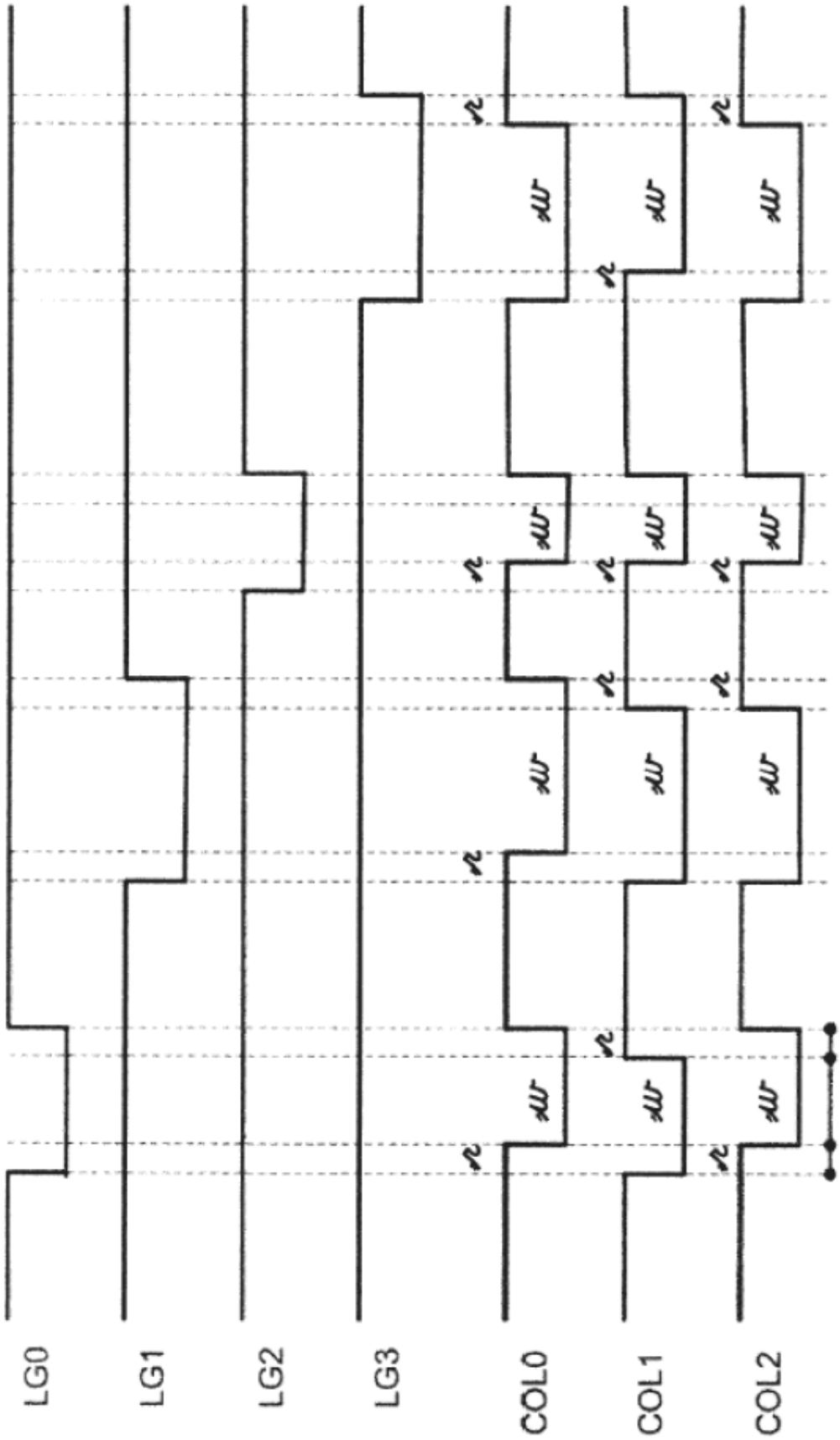

Figura 8

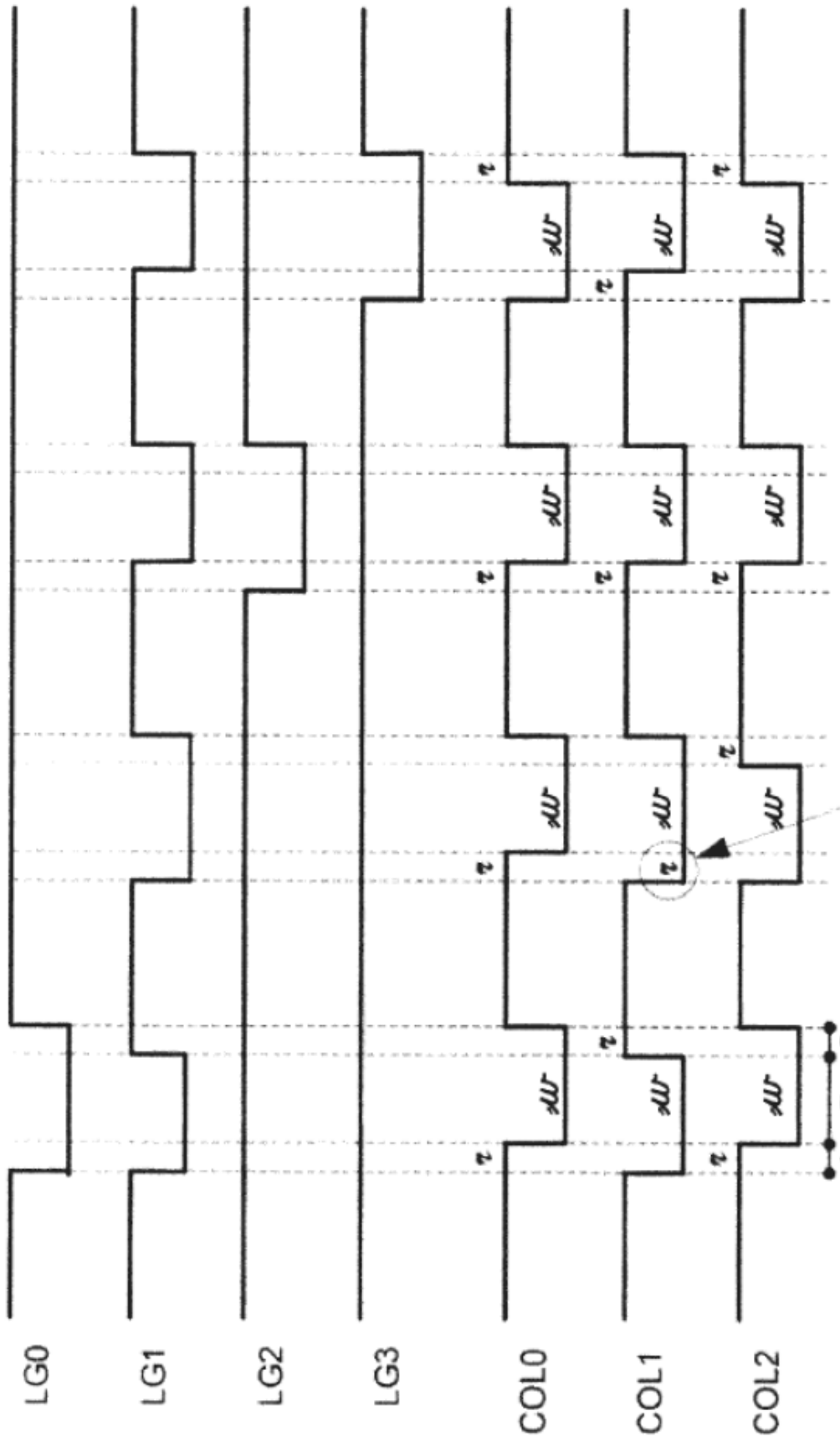
LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Detección de tecla 6
pulsada, lectura en A

Figura 9

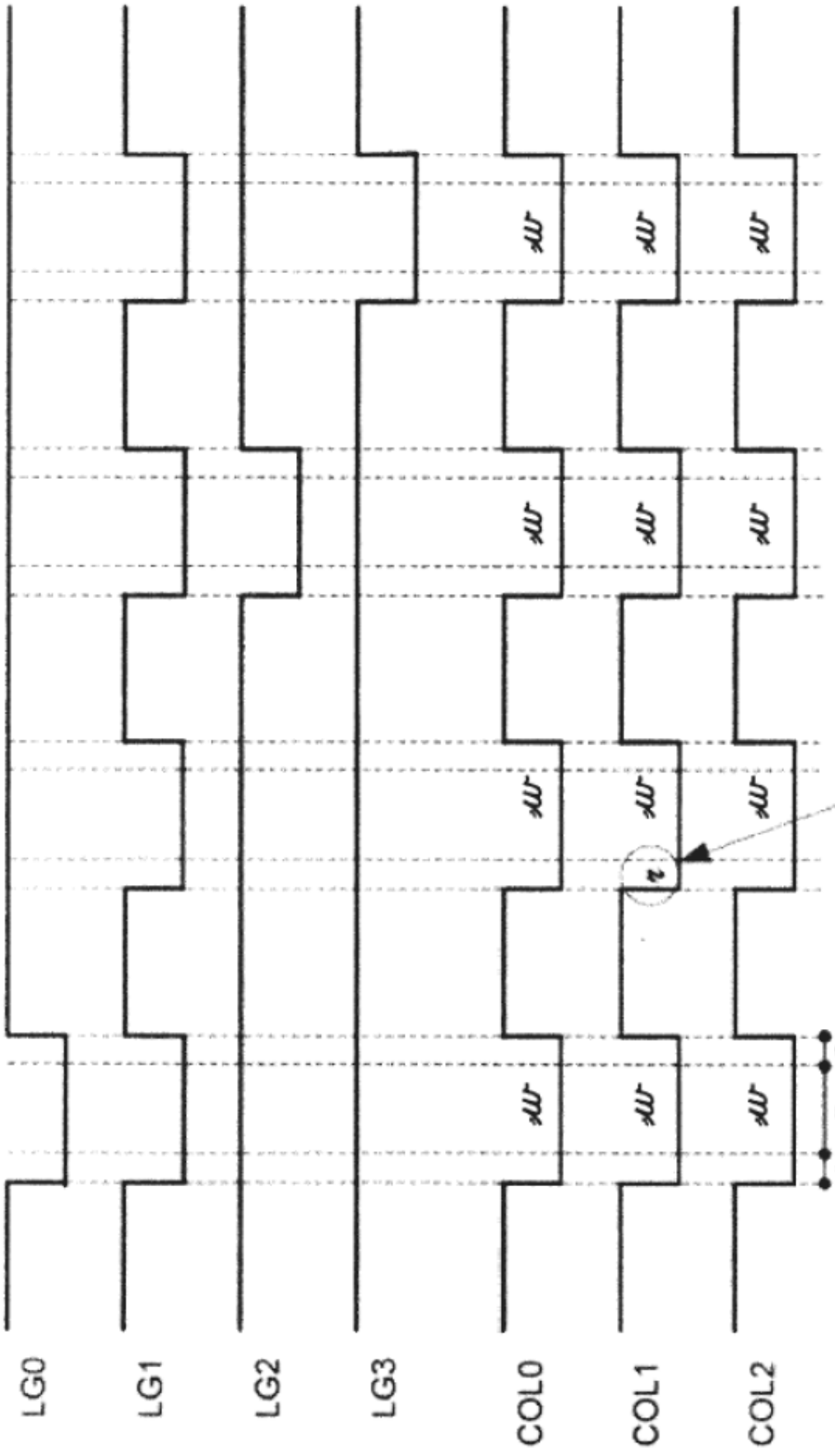
LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Confimación de detección de tecla 6 pulsada, lectura en A

Figura 10

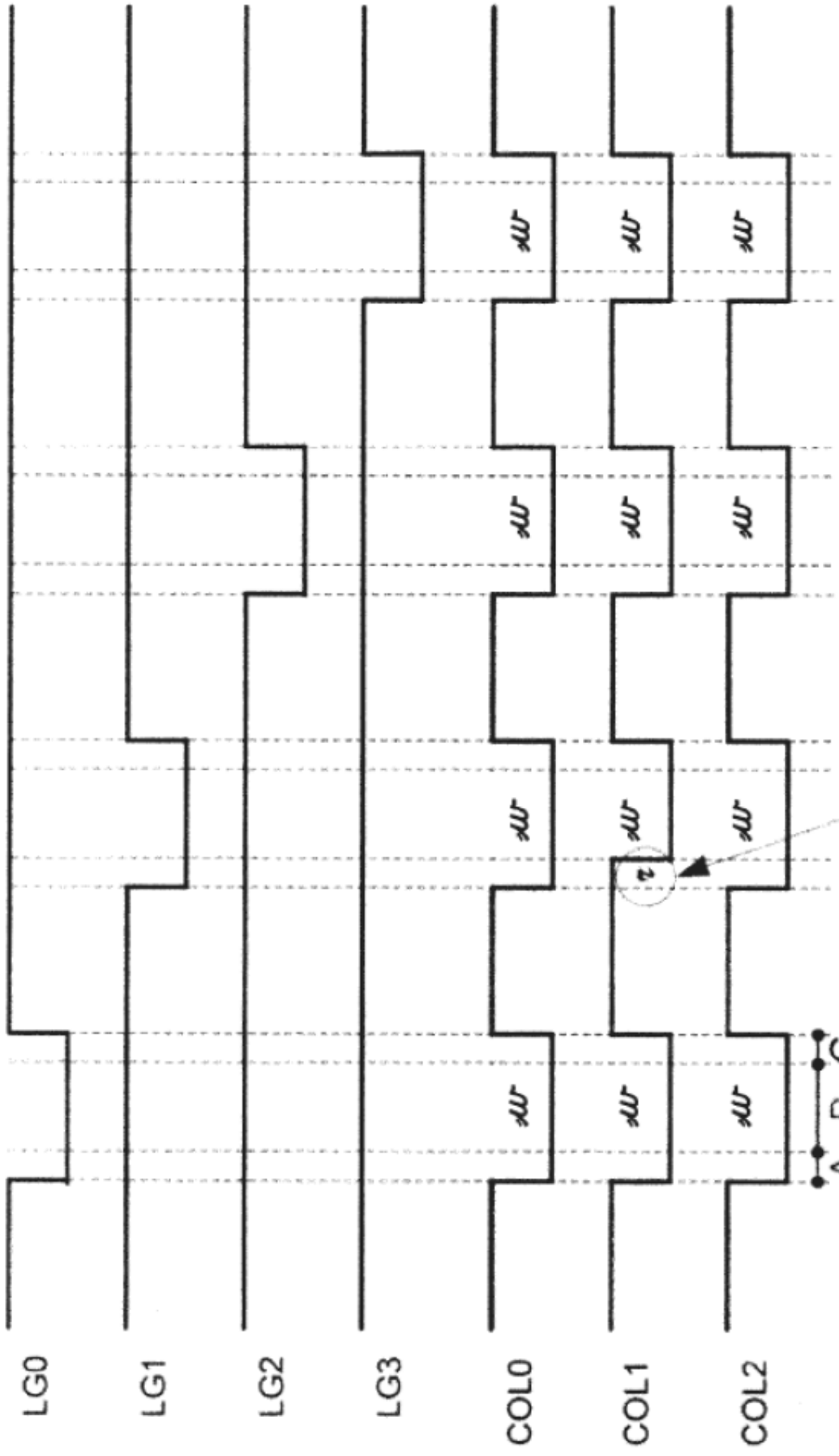
LG0
LG1
LG2
LG3
COL0
COL1
COL2
A
B
C
Detección de tecla 6 liberada,
lectura en A

Figura 11

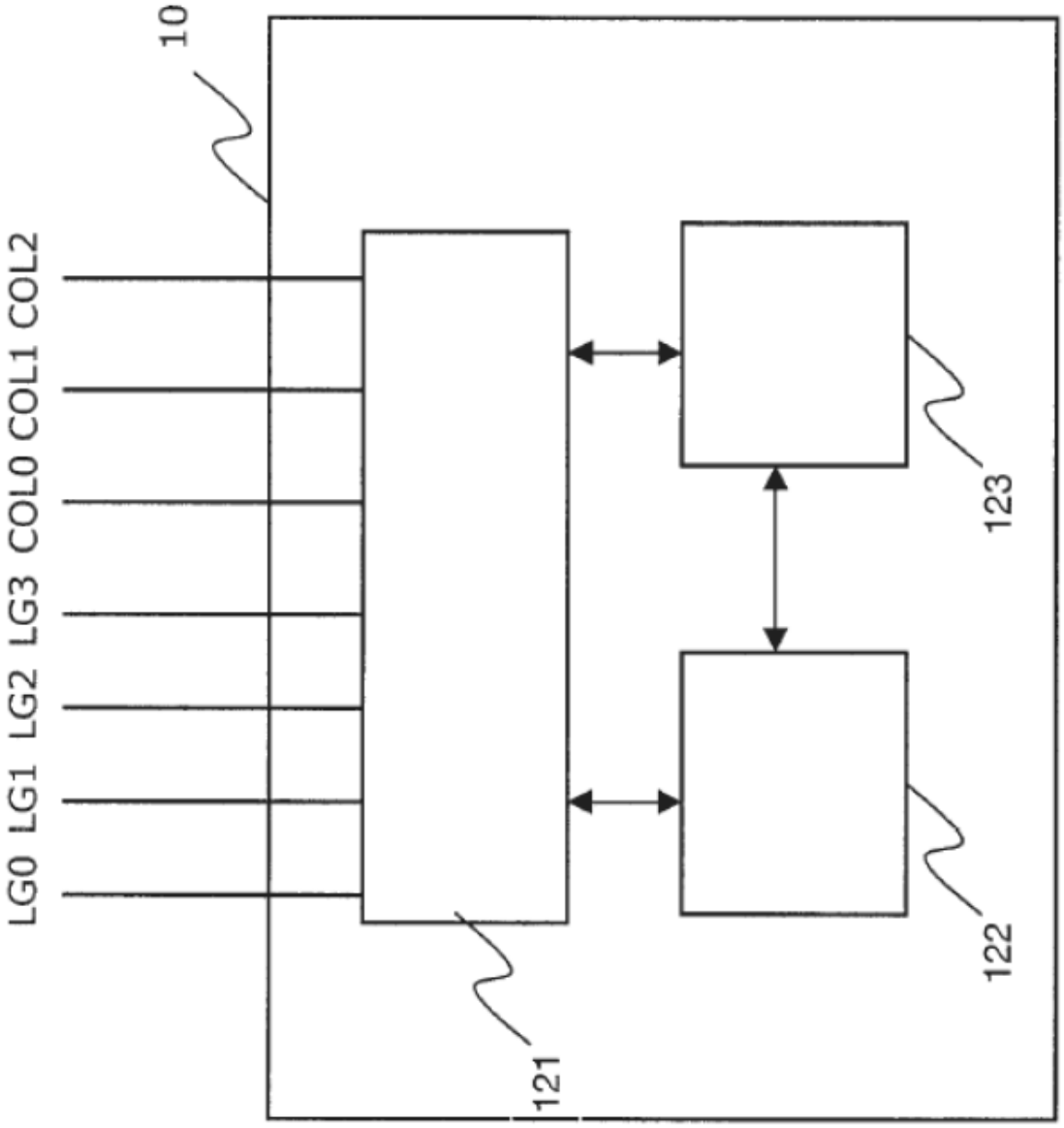

Figura 12