Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2852361 C 2019/12/31

(11)(21) 2 852 361

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2012/10/25
(87) Date publication PCT/PCT Publication Date: 2013/05/02
(45) Date de délivrance/Issue Date: 2019/12/31
(85) Entrée phase nationale/National Entry: 2014/04/15
(86) N° demande PCT/PCT Application No.: EP 2012/071189
(87) N° publication PCT/PCT Publication No.: 2013/060801
(30) Priorité/Priority: 2011/10/28 (FR1159798)

(51) Cl.Int./Int.Cl. *H03M 11/00* (2006.01),
G06F 21/83 (2013.01)

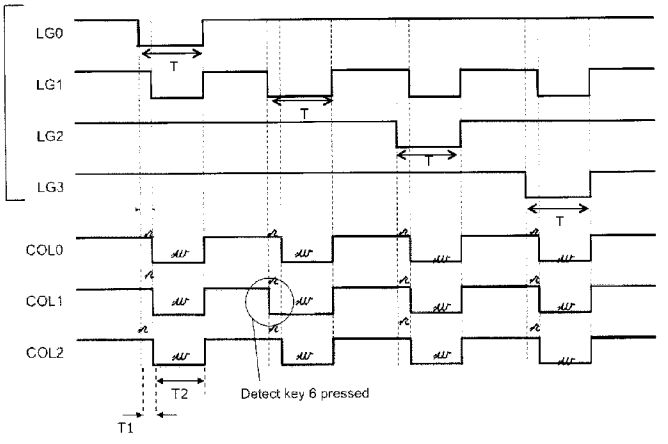
(72) Inventeurs/Inventors:
BELLAHCENE, MOHAMMED, FR;
BENOIT, OLIVIER, FR;
DELORME, JEAN-JACQUES, FR

(73) Propriétaire/Owner:
INGENICO GROUP, FR

(74) Agent: OYEN WIGGS GREEN & MUTALA LLP

(54) Titre : PROCEDE ET DISPOSITIF DE GESTION D'UNE MATRICE DE TOUCHES, PRODUIT PROG AMME D'ORDINATEUR ET MOYEN DE STOCKAGE CORRESPONDANTS

(54) Title: METHOD AND DEVICE FOR MANAGING A KEY MATRIX, CORRESPONDING COMPUTER PROGRAM PRODUCT AND STORAGE MEANS



(57) Abrégé/Abstract:
The invention relates to a method for managing, by means of a device, a matrix of keys, including at least one line (LG0 to LG3) and at least two columns (COL0 to COL2), each key making it possible to short circuit a line and a column of said matrix when pressed. The method includes at least one iteration of a sweeping phase, including the following steps for each one of the successively processed lines: writing of a predetermined logic value in the line; and for each column, reading of a logic value in the column to determine whether the column is short circuited with the line, by means of a comparison between the read logic value and the predetermined logic value. For each one of the lines processed successively: the step of writing the predetermined logic value in the line is carried out during a predetermined time interval (T); for each column, the step of reading a logic value in the column is carried out during a first portion (T1) of the predetermined time interval; the sweeping phase includes an additional step, for each column, of writing the predetermined logic value in the column, during a second portion (T2) of the predetermined time interval, the duration of the predetermined time interval being equal to the sum of the durations of the first portion and of the second portion.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
2 mai 2013 (02.05.2013)

WIPO | PCT

(10) Numéro de publication internationale
WO 2013/060801 A1

(51) Classification internationale des brevets :
H03M 11/00 (2006.01) *G06F 21/83* (2013.01)

(21) Numéro de la demande internationale :
PCT/EP2012/071189

(22) Date de dépôt international :
25 octobre 2012 (25.10.2012)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1159798 28 octobre 2011 (28.10.2011) FR

(71) Déposant : **COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO"** [FR/FR]; 28/32 Boulevard de Grenelle, F-75015 Paris (FR).

(72) Inventeurs : **BELLAHCENE, Mohammed**; 23 rue des Rancy, F-69003 Lyon (FR). **BENOIT, Olivier**; 3 rue Véronique, F-26120 Malissard (FR). **DELORME, Jean-Jacques**; 11 allée du Vallon, F-26320 Saint-Marcel-Les-Valence (FR).

(74) Mandataire : **GUENE, Patrick**; 90333, B, Technopôle Atalante, 16B rue de Jouanet, F-35703 Rennes Cedex 7 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title : METHOD AND DEVICE FOR MANAGING A KEY MATRIX, CORRESPONDING COMPUTER PROGRAM PRODUCT AND STORAGE MEANS

(54) Titre : PROCEDE ET DISPOSITIF DE GESTION D'UNE MATRICE DE TOUCHES, PRODUIT PROGRAMME D'ORDINATEUR ET MOYEN DE STOCKAGE CORRESPONDANTS

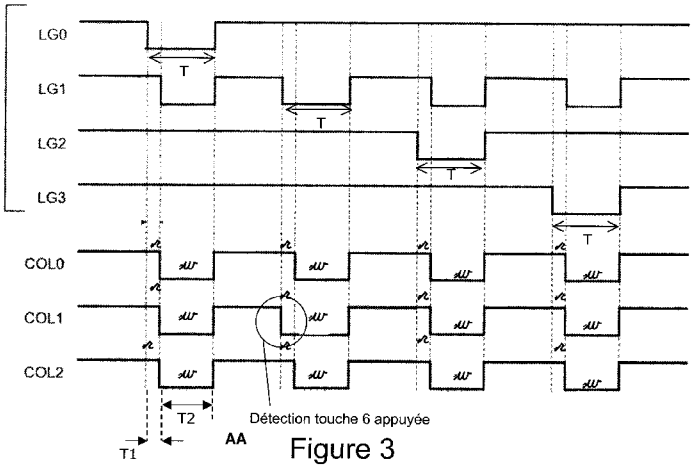


Figure 3

AA ... Detection of pressed key 6

(57) Abstract : The invention relates to a method for managing, by means of a device, a matrix of keys, including at least one line (LG0 to LG3) and at least two columns (COL0 to COL2), each key making it possible to short circuit a line and a column of said matrix when pressed. The method includes at least one iteration of a sweeping phase, including the following steps for each one of the successively processed lines: writing of a predetermined logic value in the line; and for each column, reading of a logic value in the column to determine whether the column is short circuited with the line, by means of a comparison between the read logic value and the predetermined logic value. For each one of the lines processed successively: the step of writing the predetermined logic value in the line is carried out during a predetermined time interval (T); for each column, the step of reading a logic value in the column is carried out during a first portion (T1) of the predetermined time interval; the sweeping phase includes an additional step, for each column, of writing the predetermined logic value in the column, during a second portion (T2) of the predetermined time interval, the duration of the predetermined time interval being equal to the sum of the durations of the first portion and of the second portion.

(57) Abrégé :

[Suite sur la page suivante]

WO 2013/060801 A1

WO 2013/060801 A1

GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

Il est proposé un procédé de gestion, par un dispositif, d'une matrice de touches comprenant au moins une ligne (LG0 à LG3) et au moins deux colonnes (COL0 à COL2), chaque touche permettant, quand elle est pressée, de court-circuiter une ligne et une colonne de ladite matrice. Le procédé comprend au moins une itération d'une phase de balayage comprenant les étapes suivantes pour chacune des lignes traitées successivement : écriture d'une valeur logique prédéterminée sur la ligne; et pour chaque colonne, lecture d'une valeur logique sur la colonne pour déterminer si la colonne est en court-circuit avec la ligne, par comparaison entre la valeur logique lue et la valeur logique prédéterminée, Pour chacune des lignes traitées successivement : l'étape d'écriture de la valeur logique prédéterminée sur la ligne est effectuée pendant un intervalle de temps prédéterminé (T); pour chaque colonne, l'étape de lecture d'une valeur logique sur la colonne est effectuée pendant une première partie (T1) de l'intervalle de temps prédéterminé; la phase de balayage comprend une étape supplémentaire, pour chaque colonne, d'écriture de la valeur logique prédéterminée sur la colonne, pendant une seconde partie (T2) de l'intervalle de temps prédéterminé, la durée de l'intervalle de temps prédéterminé étant égale à la somme des durées des première et seconde parties.

Method and device for managing a key matrix, corresponding computer program product and storage means.

1. FIELD OF THE INVENTION

The field of the invention is that of matrix keyboards or keypads, i.e. keypads comprising a matrix of keys enabling a user to key in or enter characters (letters, figures, symbols, etc.).

More specifically, the invention concerns a technique for the secured management of a matrix of keys such as this by a device (for example a processor) in order to determine a key or keys pressed by the user. This technique is also called a "keyboard or keypad scan routine".

The invention can be applied especially but not exclusively to the keypad of a payment terminal used to pay for purchases of goods and services. In this case, the keypad is used by the salesman to enter the amounts of the transactions and also by the customers to enter their confidential codes (PIN or Personal Identity Numbers).

The invention is not limited to a particular type of keypad and is applicable whatever the number and nature of the keys of the keypad (numerical keys, function keys, etc).

2. TECHNOLOGICAL BACKGROUND

Figure 1 shows an example of a numerical keypad comprising a matrix of keys connected to a processor 10. In this example, the matrix of keys comprises ten keys (associated with the digits 0 to 9), four rows (referenced LG0 to LG3) and three columns (referenced COL0 to COL2). Each key, when pressed, enables a row and a column of the matrix to be short-circuited. For example, when the key associated with the digit 6 is pressed, it short-circuits the row LG1 and the column COL1.

For the processor 10, the classic technique for managing a matrix of keys is to perform several successive iterations of a scan phase. As illustrated in **figure 2**, each iteration of the scan phase comprises the following steps for each of the rows LG0 to LG3 processed successively:

- writing a predetermined logic value (logic level "0" in the example of figure 2) to the row; and

– for each column COL0 to COL2, reading (symbolized by the letter "r" in figure 2) a logic value in the column to determine whether the column is short-circuited with the row, by comparison between the logic value read and the predetermined logic value.

In other words, when the processor executes an iteration of the scan phase, it writes to the rows one by one and reads the columns simultaneously. The processor can thus detect the fact that only one key has been pressed or else that several keys have been pressed simultaneously.

In the example of figure 2, and here below in the description, the writing to the rows and the reading in the columns are done at logic level "0" in assuming that the rows and the columns are at the default logic value "1". It is clear however that the principle remains the same if the use of the logic levels "0" and "1" is reversed (i.e. if the writing to the rows and the reading on the columns are done at the logic level "1" assuming that the rows and columns are at the default logic level "0").

The above formulation, which is based on a matrix of keys (matrix M) and the notion of successive writing to the rows of this matrix M and simultaneous reading in the columns of this matrix M is considered to be a generic formulation. Indeed, there is an alternative in which writing is done successively in the columns of this matrix M and reading is done simultaneously in the rows of this matrix M. However, this alternative can be performed according to the previous formulation if we consider a new matrix M' in which the rows correspond to the columns of the matrix M and the columns correspond to the rows of the matrix M.

In the example of figure 2, it is assumed that the key 6 is pressed. The processor therefore detects a short circuit between row LG1 and the column COL1 and deduces from this that the key 6 situated at the intersection between this row LG1 and this column COL1 has been pressed.

There is a need to make the classic technique for managing a matrix of keys (i.e. the classic keypad scan routine) secure.

This question is raised in the patent document FR2599525, which points to a risk that malicious individuals might try to intercept a confidential code when the operation passes from the keypad to means for the matrix analysis of the keypad, by row and by

column. Later in the description, these means are also called a device for managing the matrix of keys, or again a processor. The document FR2599525 specifies that knowledge of the waveform of the signals of analysis of the keypad enable a snooper device to immediately make a trace-back to any confidential information struck on the keypad. To snoop on the keypad, it is enough to have a few connections (through probes) on the rows and columns of the matrix of keys of the keypad. Snooping on the signals present in the rows and columns of the matrix can also be done by analysis of electromagnetic rays known as electromagnetic analysis or EMA. However, it is assumed that the signals flowing within the device for managing the matrix of keys are relatively complex, thus making it difficult for them to be used to retrieve confidential information struck on the keypad. Consequently, the device for managing the matrix of keys is called a "protected module" in the document FR2599525.

In order to improve the security of the keypad, the document FR2599525 proposes that the device for managing the matrix of keys ("protected module") should apply countermeasures to hinder the possibility of interception of any confidential information (a confidential code for example) struck on the keypad through snooping on the state of the rows and columns of the matrix of keys of the keypad.

More specifically, the technique proposed by the document FR2599525 combines the following:

- a first mechanism for simulating: the protected module is provided with two-way links towards at least certain of the columns and rows of the keypad and the protected module comprises means for simulating a false activation of keys, at least some of the interrogation pulses being applied at the same time to at least one row and at least one column;
- a mechanism for the true exploration of the keypad: the protected module explores the keypad key by key, in scrutinizing at each time a row or a column known as an "effectively analyzed" row or column, that receives no interrogation pulse (coming from the protected module). During this true exploration, the invention also proposes a complementary simulation when the protected module is in the presence of a non-transference of the start of the interrogation pulse to the column or row analyzed (i.e. one or more explored

keys are not actuated): the protected module then responds to this condition by applying a dummy pulse to the column or row analyzed which ends with the interrogation pulse (the start of this pulse being, on the contrary, slightly delayed relative to the start of the interrogation pulse, given the decision time needed for the protected module);

- a second simulation mechanism: the protected module carries out no true interrogation of a chosen key during a predetermined time corresponding to the normal time of actuation of a key and, during this same period, it creates a false response which can be attributed to this chosen key.

Two embodiments of these mechanisms are proposed.

In the first embodiment, the protected module is provided with two-way links towards all the columns of the keypad:

- for the first simulation mechanism, the protected module has a state of pure simulation in which it applies the interrogation pulse to a row and to all the columns of the keypad;
- for the mechanism of true exploration of the keypad (key by key), the protected module applies the interrogation pulse to a row and to all the columns except to an analyzed column, the key effectively explored being defined by the interrogated row and the analyzed column.

In the second embodiment, the protected module is provided with two-way links towards all the rows and all the columns of the keypad:

- for the first simulation mechanism, the protected module has a pure simulation state in which it applies the interrogation pulse to all the rows and all the columns of the keypad;
- for the mechanism of true exploration of the keypad (key by key), the protected module applies the interrogation pulse on the one hand to all the rows and columns except to an analyzed row, and, on the other hand, to all the rows and columns except to an analyzed column, the key effectively explored being defined by the row and the column analyzed.

While the technique of the document FR2599525 improves the security of the keypad, it is however not optimal. Indeed, the duration and resources of computation

needed for executing the mechanism of true exploration of the keypad are not optimized since this is a key-by-key exploration.

It will be noted that the second embodiment is even more costly in computation time and resources than the first embodiment since each key is explored in two steps, firstly through the row to which the explored key belongs and then through the column to which this explored key belongs. A greater number of sequences of interrogation signals therefore has to be generated in a same period of time so as not to lose information on the real state of the keypad.

3. GOALS OF THE INVENTION

The invention in at least one embodiment is aimed especially at overcoming these different drawbacks of the prior art.

More specifically, it is a goal of at least one embodiment of the invention, to provide a technique for the secured management, by a device (for example a processor), of a matrix of keys of a keypad.

At least one embodiment of the invention is also aimed at providing a technique of this kind enabling a faster exploration of the keypad than the technique known from the document FR2599525 discussed here above.

At least one embodiment of the invention is also aimed at providing a technique of this kind enabling an exploration of the keypad requiring fewer computation resources than the technique known from the document FR2599525 described here above.

It is another goal of at least one embodiment of the invention to provide a technique of this kind that is simple to implement and costs little.

It is another goal of the invention to render the analysis of the signals more complex for a hacker.

It is another goal of the invention to reduce the frequency of appearance of the residual signal enabling the true key pressed to be retrieved (by reducing it to the appearance and disappearance of the pressed key).

4. SUMMARY OF THE INVENTION

A preferred embodiment of the invention proposes a method for the management, by a device, of a matrix of keys comprising at least one row and at least

two columns, each key making it possible, when it is pressed, to short-circuit a row and a column of said matrix, the method comprising at least one iteration of a scan phase comprising the following steps for each of the rows processed successively: writing a predetermined logic value to the row; and for each column, reading a logic value on the column to determine whether the column is short-circuited with the row by comparison between the logic value read and the predetermined logic value. For each of the rows processed successively:

- the step for writing the predetermined logic value on the row is performed during a predetermined time slot;
- for each column, the step for reading a logic value on the column is performed during a first part of the predetermined time slot;
- the scan phase comprises an additional step, for each column, for writing the predetermined logic value to the column during a second part of the predetermined time slot, the duration of the predetermined time slot being equal to the sum of the duration of the first and second parts.

In other words, during this predetermined time slot (T), for each of said columns:

* the step for reading a logic value in the column is performed during a first part (T1) of said predetermined time slot (T);
* the scan phase comprises an additional step for writing the predetermined logic value to the column during a second part (T2) of said predetermined time slot (T), the duration of said predetermined time slot (T) being equal to the sum of the durations of the first and second parts.

Thus, the device (which manages the matrix of keys of the keypad) implements a first countermeasure aimed at making the signals present in the columns as independent as possible of the key or keys pressed, while at the same time reducing the duration of exploration of the keypad. To this end, for a given row to which it writes during a time slot T, the device reads and writes on each column: reading during T1 and writing during T2, with: T1 + T2 = T. Hence, unlike in the technique known from the document FR2599525 (which proposes a key-by-key exploration), the device of the invention simultaneously explores all the keys associated with a same row.

Thus, if the key associated with a given row is pressed, only the signal present in the column associated with this key is slightly different from the signals present in the other columns. This signal does not have the same value as the others during T1 since it takes the predetermined logic value written to the given row. However, it is identical to the other signals during T2 since the predetermined logic value is written to all the columns. In other words, within a time slot T:

- if no key is pressed, the signal edges indicating the passage of a predetermined logic value (start of T2) are synchronous for all the columns;
- if a key is pressed, the signal edges indicating the passage to a predetermined logic value (start of T2) are synchronous for all the columns except for the column associated with the key pressed (for this column, this signal edge corresponds to the start of T1, and is therefore in advance relative to the synchronous edges of the other columns).

The above formulation, which is based on a matrix of keys (matrix M) and the notions of successive operations of writing (during T) to each of the rows of this matrix M and operations of reading (during T1) and writing (during T2) to each of the columns of this matrix M, is generic. Indeed, there is an alternative which consists in successively writing (during T) to each of the columns of this matrix M and in reading in (during T1) and writing (during T2) to each of the rows of this matrix M. However, this alternative can be processed according to the previous formulation if we consider a new matrix M' in which each of the rows corresponds to the columns of the matrix M and the columns correspond to the rows of the matrix M.

According to one particular aspect of the invention, for each column, the order of steps for reading and writing during the predetermined time slot is selected randomly.

In other words, for each column, the device makes a random choice between: a reading during T1 and then a writing during T2 or else a writing during T2 and then a reading during T1.

Thus, the device (which manages the matrix of keys of the keypad) implements a second countermeasure in combination with the first countermeasure. This second countermeasure is aimed at making it more difficult to detect a pressed key. The random aspect also prevents any learning by a snooper device. Indeed, within a time slot T:

- if no key is pressed, the signal edges indicating the passage to the predetermined logic value (start of T2) are not synchronous for all the columns because the order between the reading and writing (i.e. between T1 and T2) is not the same for all the columns;
- if a key is pressed, the signal edges indicating the passage to the predetermined logic value (start of T2) are not synchronous either for all the columns (for the column associated with the pressed key, this signal edge is not easy to locate by simple comparison with the synchronous edges of the other columns).

Advantageously, in each predetermined time slot, the duration of the second part of the predetermined time slot is identical for all the columns.

In this way, the resemblance between the signals present in the different columns is increased and the detection of a pressed key is made even more difficult.

According to one particular characteristic, the matrix of keys comprises a plurality of rows and, at each iteration of the scan phase, the order of successive processing of the rows is random.

Thus, the device (which manages the matrix of keys of the keypad) implements a third countermeasure used to further increase the complexity of the analysis of the signals present in the rows and columns that must be made by a snooper device to determine any confidential information struck on the keys of the keypad.

According to one particular aspect of the invention, the matrix of keys comprises a plurality of rows and during a given iteration of the scan phase, at least one parameter varies randomly from one row to the other, said at least one parameter belonging to the group comprising:

- the duration of the predetermined time slot;
- the duration of the first part of the predetermined time slot; and
- the duration of the second part of the predetermined time slot.

Thus, the device (which manages the matrix of keys of the keypad) implements a fourth countermeasure to further increase the complexity of analysis of the signals present in the rows and in the columns.

According to one particular characteristic, at least one iteration of the scan phase, which follows an iteration during which at least one short-circuit has been determined between a given column and a given row, comprises the following steps;

- for each of the successively processed rows, other than a given row that is short-circuited with a given column:
  * for each column, writing the predetermined logic value to the column throughout the duration of the time slot;
- for each given row short-circuited with a given column:
  * for each column other than the given column, writing the predetermined logic value to the column throughout the duration of the time slot; and
  * for the given column, reading a logic value during the first part of the time slot in order to detect a continuing or a stopping of said short-circuit between the given column and the given row, and writing the predetermined logic value during the second part of the time slot.

Thus, the device (which manages the matrix of keys of the keypad) implements a fifth countermeasure enabling the concealment of a pressure on one (or more) keys. Indeed, as soon as pressure on a key has been detected during the iteration of the scan phase, the behavior of the device in the next iterations of the scan phase is such that, so long as this key is pressed, the signals present in all the columns are identical (predetermined logic value during T). It is therefore only during two iterations (that of the detection of the key pressed and that of the detection of the release of the key) that a snooper device can know if the key has been pressed. On the other hand, however, pressure on another key cannot be detected until the detection of the release of the pressed key is iterated. It is also possible to manage simultaneous keys if they appear at the same time and in one and the same detection phase which is extremely improbable in practice.

Another embodiment of the invention proposes a computer program product comprising program code instructions for implementing the above-mentioned method (in any one of its different embodiments) when said program is executed on a computer or a processor.

Another embodiment of the invention proposes a computer-readable and non-transient storage medium storing a computer program comprising a set of instructions executable by a computer or a processor to implement the above-mentioned method (in any one of its different embodiments).

Another embodiment of the invention proposes a device for managing a matrix of keys comprising at least one row and at least two columns, each key making it possible, when it is pressed, to short-circuit a row and a column of said matrix, the device comprising means for scanning adapted to carrying out at least one iteration of a scan phase, the means for scanning comprising the following means, activated for each of the rows processed successively: means for writing a predetermined logic value to the row; and means for reading a logic value on each column to determine whether the column is shorted-circuited with the row, by comparison between the logic value read and the predetermined logic value. For each of the rows processed successively, the means for writing the predetermined logic value to the row are activated during a predetermined time interval; for each column, the means for reading a logic value on the column are activated during a first part of the predetermined time interval. The means for scanning comprise additional means for writing, activated for each column during a second part of the predetermined time slot to write the predetermined logic value to the column, the duration of the predetermined time slot being equal to the sum of the durations of the first and second parts.

In other words, the means for scanning comprise additional means for writing and, for each of the rows processed successively:

- the means for writing the predetermined logic value to the row are activated during a predetermined time slot (T);
- during said predetermined time slot (T), for each of said columns:
  * the means for reading the logic value on the column are activated during a first part (T1) of said predetermined time slot (T);
  * the additional means for writing are activated during a second part (T2) of said predetermined time slot (T) to write the predetermined logic value to the column, the duration of the predetermined time slot being equal to the sum of durations of the first and second parts.

Advantageously, the device for managing the matrix of keys comprises means for implementing steps that it performs with the method as described here above in any one of its different embodiments.

5. LIST OF FIGURES

Other features and characteristics of the invention shall appear from the following description, given by way of an indicative and non-exhaustive example, and from the appended figures, of which:

- Figure 1, already described with reference to the prior art, presents an example of a numerical keypad comprising a matrix of keys connected to a processor;
- Figure 2, already described with reference to the prior art, illustrates the classic technique of management of the matrix of keys of figure 1, when the key 6 is pressed;
- Figure 3 illustrates a first countermeasure, according to one particular embodiment of the invention, when the key 6 is pressed;
- Figures 4, 5 and 6 illustrate a combination of the first countermeasures with a second countermeasure, according to one particular embodiment of the invention (no key pressed in figure 4; key 6 pressed and detected in the time slot A, in figure 5, and in the time slot C, in figure 6);
- Figure 7 illustrates a third countermeasure, capable of being combined with the first countermeasure (and any one of the other countermeasures);
- Figure 8 illustrates a combination of the first and second countermeasures with a fourth countermeasure, according to a particular embodiment of the invention (no key is pressed);
- Figures 9, 10 and 11 illustrate a combination of the first and second countermeasures with a fifth countermeasure, according to one particular embodiment of the invention (first detection of the key 6 pressed, in figure 9; confirmation of the detection of the key 6 pressed, in figure 10; detection of the key 6 released, in figure 11); and
- Figure 12 presents the structure of a device for managing a matrix of keys of a keypad, according to one particular embodiment of the invention.

6. DETAILED DESCRIPTION

For the sake of simplification, here below in the description we use the example of the keypad of figure 1 with a matrix of keys comprising ten keys (associated with the digits 0 to 9), four rows (referenced LG0 to LG3) and three columns (referenced COL0 to COL2). It is clear that the countermeasures presented here below according to different embodiments of the invention are not limited to this example of a keypad.

Each of the figures 3 to 6 and 8 to 11 has logic values present in the rows LG0 to LG3 and the columns COL0 to COL2 during an iteration of the scan phase. The figure 7 presents the logic values present in the rows LG0 to LG3 during two iterations of the scan phase.

It is assumed that the interrogation pulses have a logic level "0". It is clear that the principle remains the same if the use of the logic levels "0" and "1" is reversed.

Referring now to **figure 3**, we present a first countermeasure according to one particular embodiment of the invention. It is assumed that the key 6 is pressed.

During the time interval T for writing an interrogation pulse (logic level "0") to each of the rows LG0 to LG3, the processor performs the following steps for each column COL0 to COL2:

- reading (symbolized by the letter "r" in figure 3) of a logic value on the column during a first part T1 of the time slot T to determine (by comparison between the logic value read and the logic value "0") whether the column is short-circuited with the row;
- writing (symbolized by the letter "w" in figure 3) of a logic value "0" to the column during a second part T2 of the time slot T (with the duration of T being equal to the sum of the durations of T1 and T2).

Thus, in the iteration of the scan phase presented in the figure 3, each of the rows LG0 to LG3 can take one of the following states:

- outside the time slot T, a state "not enforced by the processor" in which the row takes:
  - * the default logic value "1" if this row is not short-circuited with a column; or

* the logic value of a given column, if this row is short-circuited with this given column (i.e. if the key associated with this row and this column is pressed);

- during the time slot T, a state "enforced by the processor" in which the row takes the logic value "0" written by the processor.

Similarly, in the iteration of the scan phase presented in figure 3, each of the columns COL0 to COL2 can take one of the following states:

- outside the time slot T, a state "not enforced by the processor" in which the column takes the default logic value "1";
- during the first part T1 of the time slot T, a state "not enforced by the processor" (the processor reads this column) in which the column takes:
  - the default logic value "1" if this column is not short-circuited with the row to which the processor has written the value "0"; or
  - the logic value "0" if this column is short-circuited with a row to which the processor has written the value "0";
- during the second part T2 of the time slot T, a state "enforced by the processor" in which the column takes the logic value "0" written by the processor.

In the example of figure 3, the key 6 (associated with the row LG1 and the column COL1) is pressed. Hence, for each of the columns COL0 and COL2, the processor reads the logic value "1" during each first part T1 of the time slot T and writes the value "0" during each second part T2 of the time slot T. For the column COL1, the processor acts in the same way except for the time slot T for writing to the row LG1 during which the processor reads the logic value "0" during the first part T1 of this time slot (because the row LG1 is short-circuited with the column COL1) and writes the value "0" during the second part T2 of this time slot. It will be noted that, because the key 6 is pressed, the value of the row LG1 follows that of the column COL1.

A "non-enforced" state for a row or column corresponds to a port of the processor connected to this row or column and is configured at input with a pull-up

resistor or pull-down resistor, this pull-up or pull-down resistor setting the electrical level.

An "enforced" state for a row or column corresponds to a port of the processor connected to this row or column and configured at output at a logic level "1" or "0".

The first countermeasure presented here above is vulnerable to a detailed analysis of the signals present on the columns COL0 to COL2 since it can be noted that, for the pair (LG1, COL1), the trailing edges are synchronous whereas for the other pairs (row, column), the trailing edge of the column signal is offset (by T1) relative to the trailing edge of the row signal.

Figures 4, 5 and 6 present a combination of the first countermeasure with a second countermeasure according to one particular embodiment of the invention.

In order to overcome the weakness of the first countermeasure, it is combined with the second countermeasure in which the processor 10 randomly selects the order of the reading operations (during T1) and writing operations (during T2) for each column COL0 to COL2.

Furthermore, during each time slot T, the duration of T2 (of writing by the processor) is identical for all the columns.

In figures 4, 5 and 6, each time slot T (for writing an interrogation pulse to a row) is sub-divided into three portions named A, B and C respectively. For each COL0 to COL2, we have either: T1 = A and T2 = B + C (i.e. reading in A and writing to B and C), and: T1 = C and T2 = A + B (i.e. reading in C and writing to A and B).

In the example of figures 4 and 6, we have:

- T1 = A and T2 = B + C, for the following pairs: (LG0, COL0), (LG0, COL2), (LG1, COL0), (LG2, COL0), (LG2, COL1), (LG2, COL2) and (LG3, COL1);
- T1 = C and T2 = A + B, for the following pairs: (LG0, COL1), (LG1, COL1), (LG1, COL2), (LG3, COL0) and (LG3, COL2).

The example of figure 5 can be distinguished from that of figures 4 and 6 only for the pair (LG1, COL1), for which we have: T1 = A and T2 = B + C (i.e. reading in A instead of reading in C).

The following assumptions are made: no key is pressed in figure 4. In figure 5, the key 6 is pressed and hence detected in the portion A. In figure 6, the key 6 is pressed and hence detected in the portion C.

Referring now to **figure 7**, we present a third countermeasure according to one particular embodiment of the invention. It can be combined with the first countermeasure (alone or in combination with any one of the other countermeasures).

In order to further increase the complexity of the analysis of the signals of the columns and make the method implemented by the processor even less predictable, the third countermeasure consists of a random choice of the order in which the processor writes the interrogation pulse on the rows, at each iteration of the scan phase.

In the example of figure 7, in a first iteration referenced 71, the processor writes to the rows in the following order: LG1, LG0, LG3 and LG2. In another iteration referenced 72, the processor writes to the rows in the following order: LG2, LG1, LG3 and LG0.

Referring now to **figure 8**, we present a combination of the first and second countermeasures with a fourth countermeasure.

In the fourth countermeasure, the processor makes one or more of the following parameters vary randomly from one row to another at each iteration of the scan phase:

- the duration of the predetermined time slot T;
- the duration of the first part T1 (reading by the processor) of the time slot T; and
- the duration of the second part T2 (writing by the processor) of the time slot T.

Thus, snooping with activation on a specific width is prevented.

In the example of figure 8, only the duration of the portion B varies randomly, hence the duration of the predetermined time slot T also varies randomly (i.e. the case of the duration of the second part T2, since T2 is equal to A+B or B+C). By contrast, the duration of the first part T1 is not variable in this example (since T1 is equal to A or C).

Referring now to **figures 9, 10 and 11**, we present a combination of the first and second countermeasures with a fifth countermeasure according to one particular embodiment of the invention.

In the fifth countermeasure, once a pressed key has been detected during an iteration of the scan phase (here below called an iteration of detection of pressing), this pressed key is concealed during the following iterations of the scan phase (here below called iterations of confirmation of pressing), until there is a detection of a release of this key during an iteration of a scan phase (here below called an iteration of detection of release).

Figure 9 presents an example of an iteration of detection of pressing in which a pressing of the key 6 is detected (reading at A of the logic value "0" and then reading at B and C of the logic value "0" for the pair (LG1, COL1)). This figure 9 is identical to figure 5 and is not described again.

Figure 10 presents an example of an iteration of confirmation of pressing, in which the pressing of the key 6 is confirmed (for the pair (LG1, COL1)) reading in A of the logic value "0" then writing of the logic value "0" to B and C, i.e. T1=A and T2=B+C). In order to conceal the pressure on this key 6, for all the other pairs (row, column), the processor does not read the columns but writes only the logic value "0" throughout the duration of the time slot T of the interrogation pulse (writing during A, B and C, i.e. T2=A+B+C=T). Thus, for each time slot T, all the signals present on the different columns are strictly identical (logic value "0" during T).

Figure 11 presents an example of an iteration of detection of release, in which the release of the key 6 is detected (for the pair (LG1, COL1), reading in A of the logic value "1" and then writing of the logic value "0" to B and C, i.e. T1=A and T2=B+C).

Figure 12 presents a structure of a device 10 for managing a matrix of keys of a keypad according to one particular embodiment of the invention. This device implements the countermeasures presented here above or a combination of certain of these countermeasures.

In this example, the device comprises a RAM (random access memory) 123, a central processing unit or CPU 121, equipped for example with a processor and driven by a program stored in the ROM (read-only memory) 122. At initialization, the code instructions of the program are for example loaded into the RAM 123 and then executed by the processing unit 121. The processing unit 121 manages the signals on the rows

and columns (LG0 to LG3 and COL0 to COL2 in this example) of the matrix of keys of the keypad according to the instructions of the program 122, in order to implement the totality or a part of the countermeasures described in detail further above.

This figure 12 illustrates only one particular way, among several possible ways, of carrying out the different countermeasures described in detail here above with reference to figures 3 to 11. Indeed, the technique of the invention can be done equally well:

- on a reprogrammable computing machine (a processor or a microcontroller for example) executing a program comprising a sequence of instructions, or
- a dedicated computing machine (for example a set of logic gates such as an FPGA or an ASIC, or any other hardware module).

Should the invention be implanted in a reprogrammable computing machine, the corresponding program (i.e. the sequence of instructions) can be stored in a detachable storage medium (such as for example a floppy disk, a CD-ROM or a DVD-ROM) or non-detachable storage medium, this storage medium being partially or totally readable by a computer or a processor.

CLAIMS

1. Method for the management, by a device (10), of a matrix of keys comprising at least one row (LG0 to LG3) and at least two columns (COL0 to COL2), each key making it possible, when it is pressed, to short-circuit a row and a column of said matrix, the method comprising at least one iteration of a scan phase comprising the following steps for each of the rows processed successively:

- writing a predetermined logic value to the row; and
- for each column, reading a logic value on the column to determine whether the column is short-circuited with the row, by comparison between the logic value read and the predetermined logic value,

characterized in that, for each of the rows processed successively:

- the step for writing the predetermined logic value to the row is performed during a predetermined time slot (T)) ;
- during said predetermined time slot (T), for each of said columns:
  * the step for reading a logic value on the column is performed during a first part (T1) of said predetermined time slot (T);
  * the scan phase comprises an additional step for writing the predetermined logic value to the column during a second part (T2) of said predetermined time slot (T), the duration of said predetermined time slot (T) being equal to the sum of the durations of the first and second parts.

2. The method according to claim 1, characterized in that, for each column, the order of steps for reading and writing during the predetermined time slot is selected randomly.

3. The method according to claim 2, characterized in that, in each predetermined time slot, the duration of the second part of the predetermined time slot is identical for all the columns.

4. The method according to any one of the claims 1 to 3, characterized in that the matrix of keys comprises a plurality of rows and, at each iteration of the scan phase, the order of successive processing of the rows is random.

5. The method according to any one of the claims 1 to 4, characterized in that the matrix of keys comprises a plurality of rows and, in that, during a given iteration of the

scan phase (71, 72), at least one parameter varies randomly from one row to the other, said at least one parameter belonging to the group comprising:

- the duration of the predetermined time slot;
- the duration of the first part of the predetermined time slot; and
- the duration of the second part of the predetermined time slot.

6. The method according to any one of the claims 1 to 5, characterized in that, at least one iteration of the scan phase, which follows an iteration during which at least one short-circuit has been determined between a given column and a given row, comprises the following steps:

- for each of the successively processed rows, other than a given row that is short-circuited with a given column:
  - * for each column, writing the predetermined logic value to the column throughout the duration of the time slot;
- for each given row short-circuited with a given column:
  - * for each column other than the given column, writing the predetermined logic value to the column throughout the duration of the time slot; and
  - * for the given column, reading a logic value during the first part of the time slot in order to detect a continuing or a stopping of said short-circuit between the given column and the given row, and writing the predetermined logic value during the second part of the time slot.

7. Computer-readable and non-transient storage medium storing a computer program comprising a set of instructions executable by a computer or a processor to implement the method according to any one of the claims 1 to 6.

8. Device for managing a matrix of keys comprising at least one row and at least two columns, each key making it possible, when it is pressed, to short-circuit a row and a column of said matrix, the device comprising means for scanning adapted to carrying out at least one iteration of a scan phase, the means for scanning comprising the following means, activated for each of the rows processed successively:

- means for writing a predetermined logic value to the row; and

- means for reading a logic value on each column to determine whether the column is shorted-circuited with the row, by comparison between the logic value read and the predetermined logic value,

characterized in that the means for scanning comprise additional means for writing, and in that, for each of the rows processed successively:

- the means for writing the predetermined logic value to the row are activated during a predetermined time slot (T);
- during said predetermined time slot (T), for each of said columns:
  * the means for reading the logic value on the column are activated during a first part (T1) of said predetermined time slot (T);
  * the additional means for writing are activated during a second part (T2) of said predetermined time slot (T) to write the predetermined logic value to the column, the duration of the predetermined time slot being equal to the sum of durations of the first and second parts.

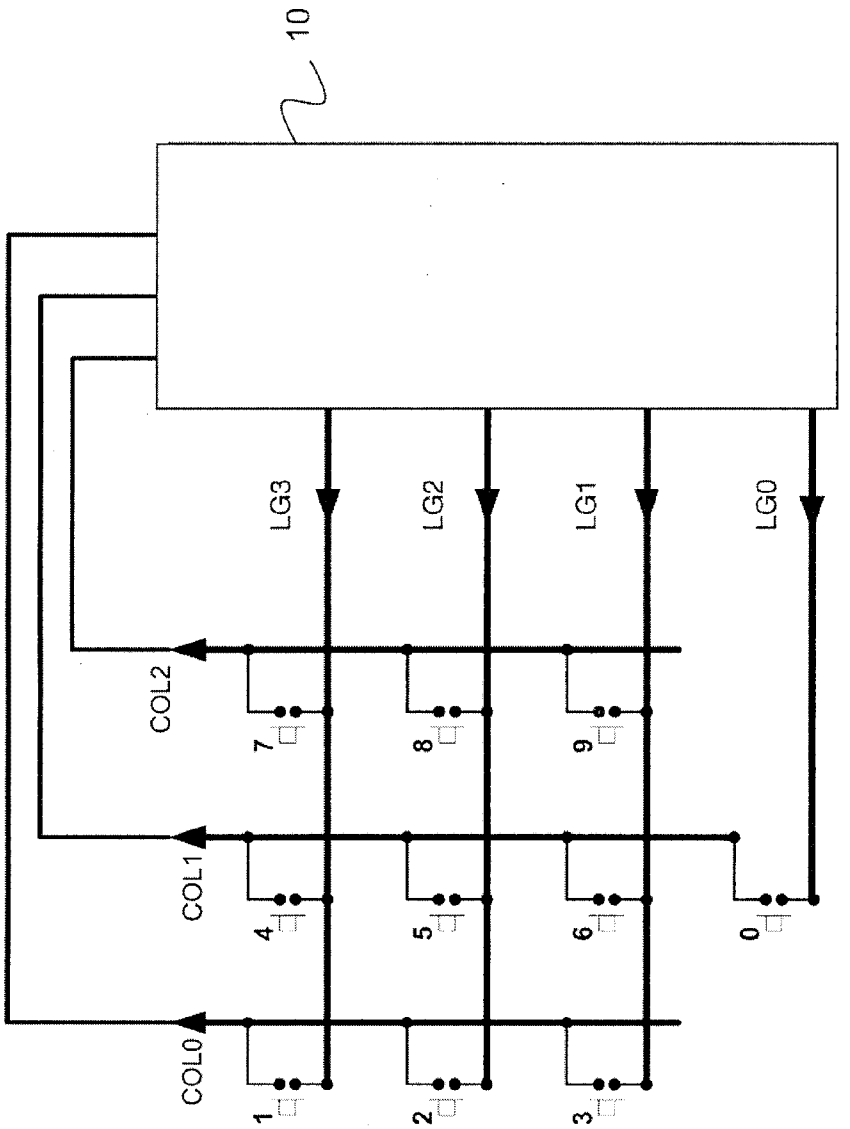


Figure 1

PRIOR ART

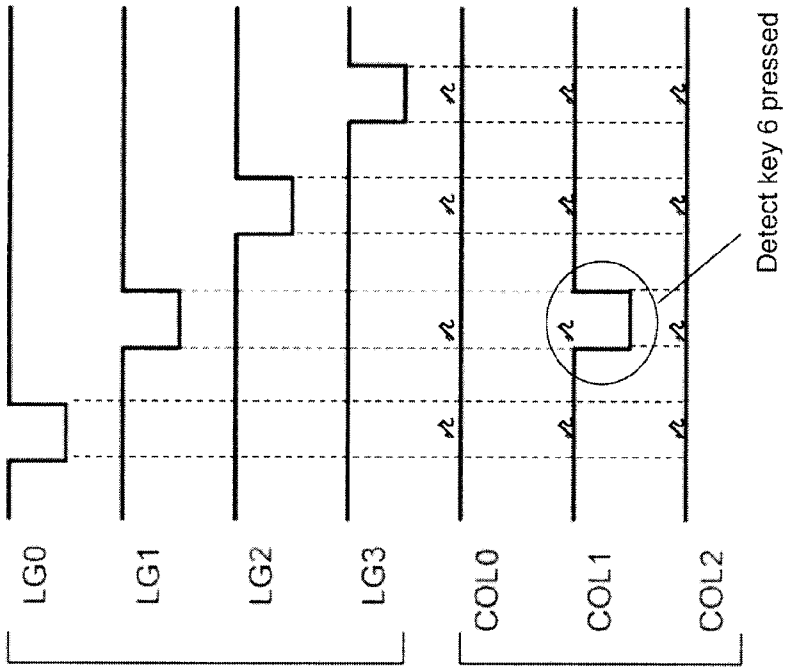


Figure 2

PRIOR ART

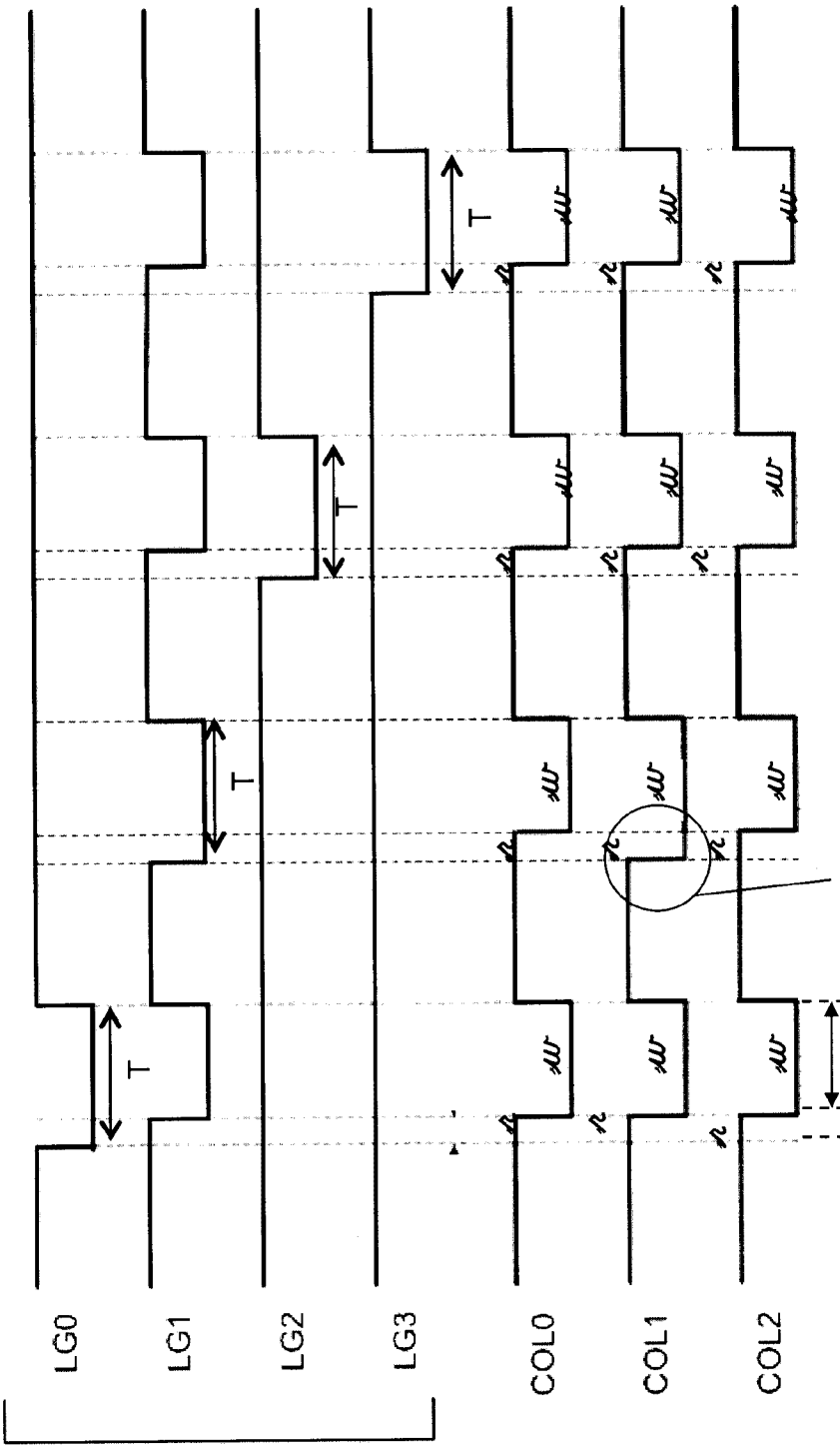


Figure 3

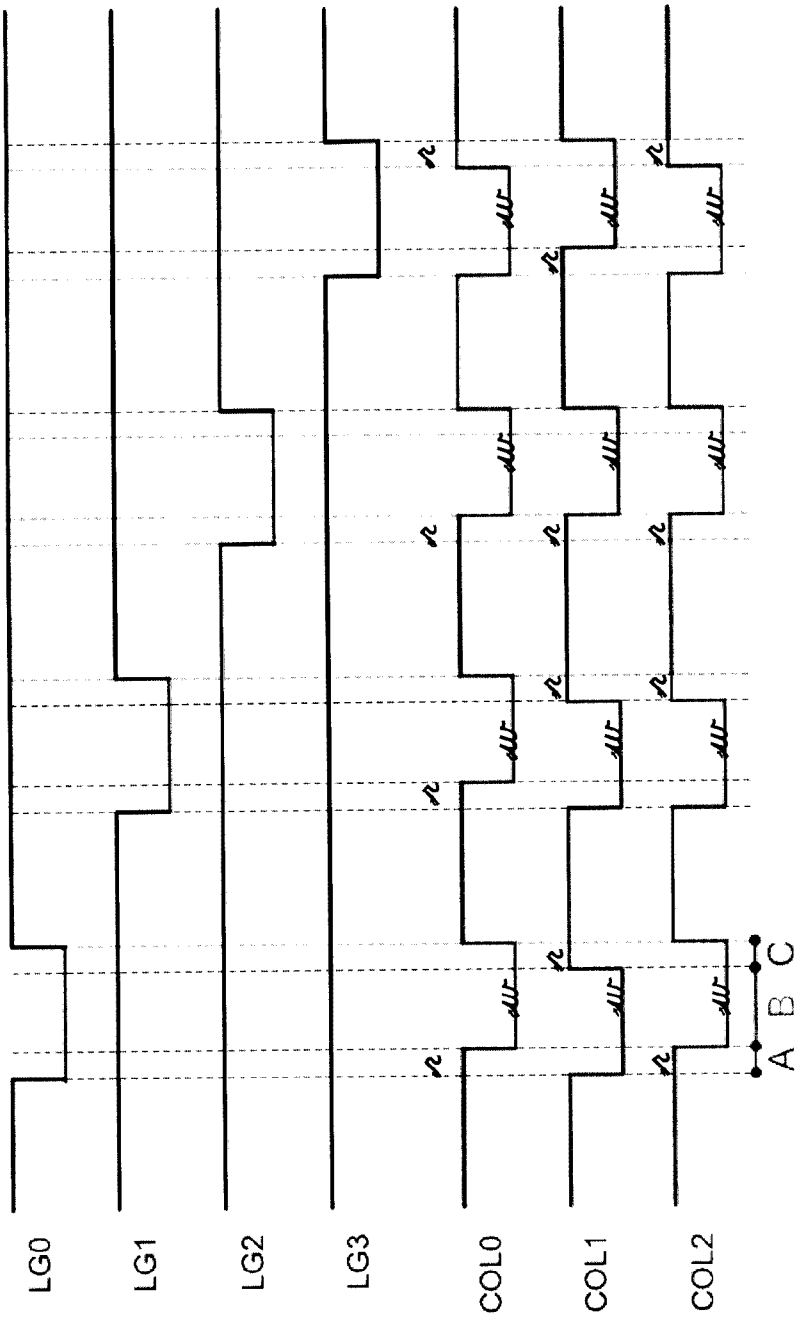


Figure 4

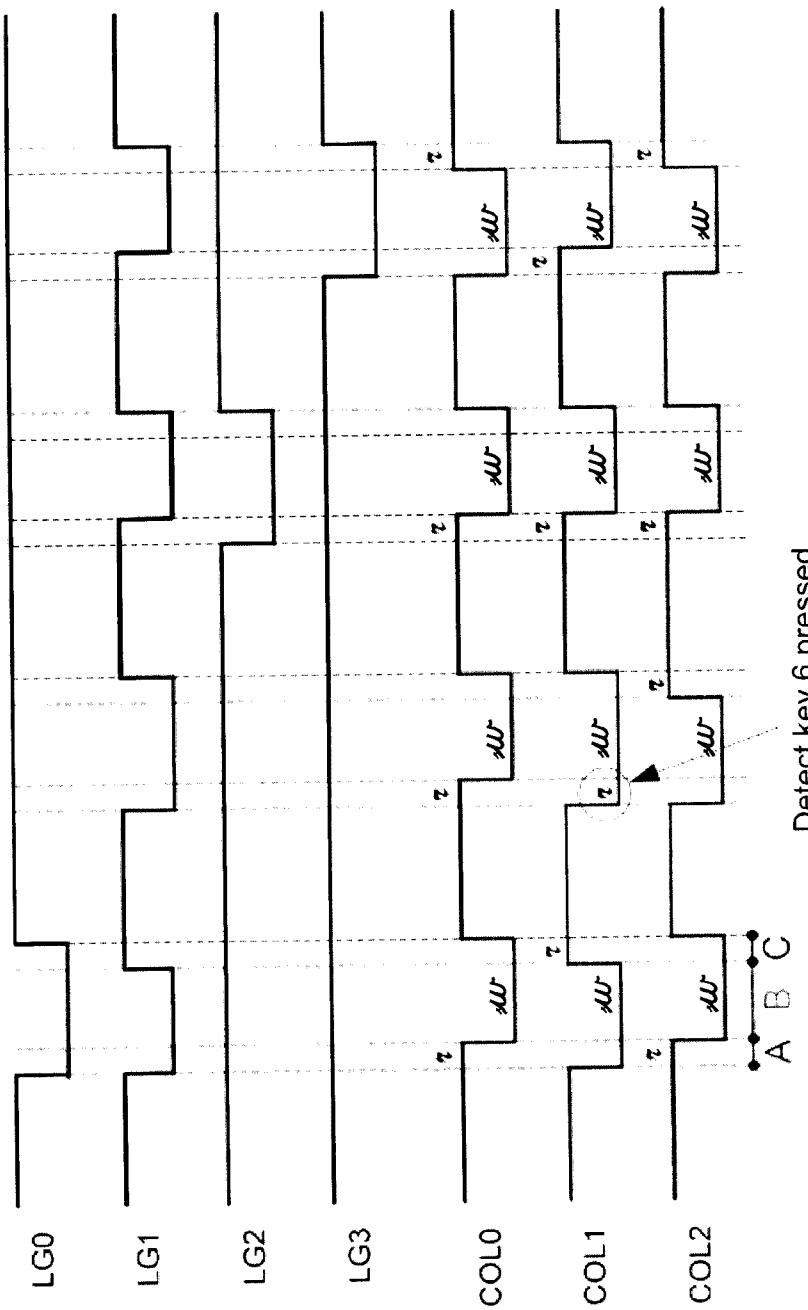

LG0
LG1
LG2
LG3
COL0
COL1
COL2
A
B
C
Detect key 6 pressed, reading in A

Figure 5

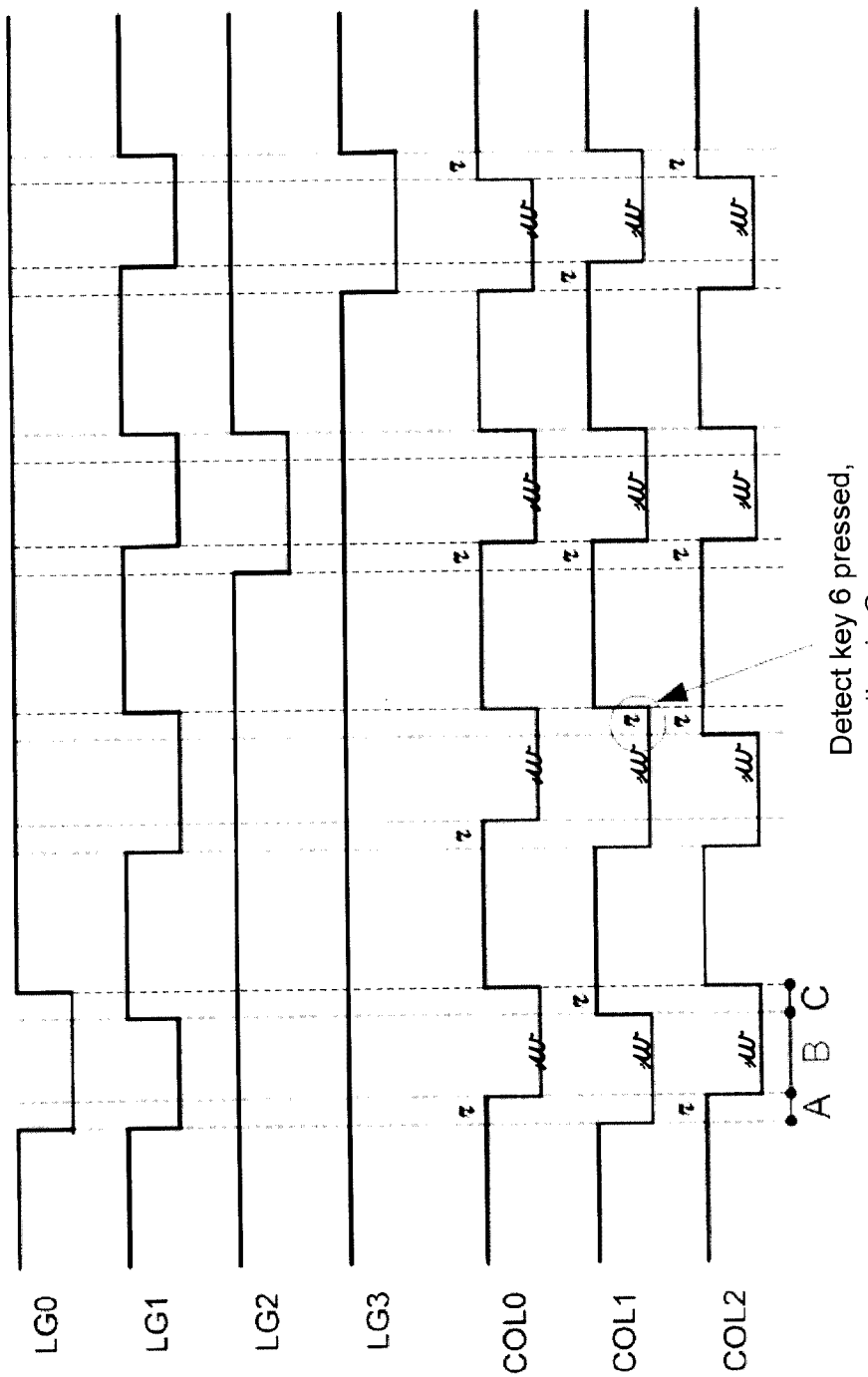

LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Detect key 6 pressed, reading in C

Figure 6

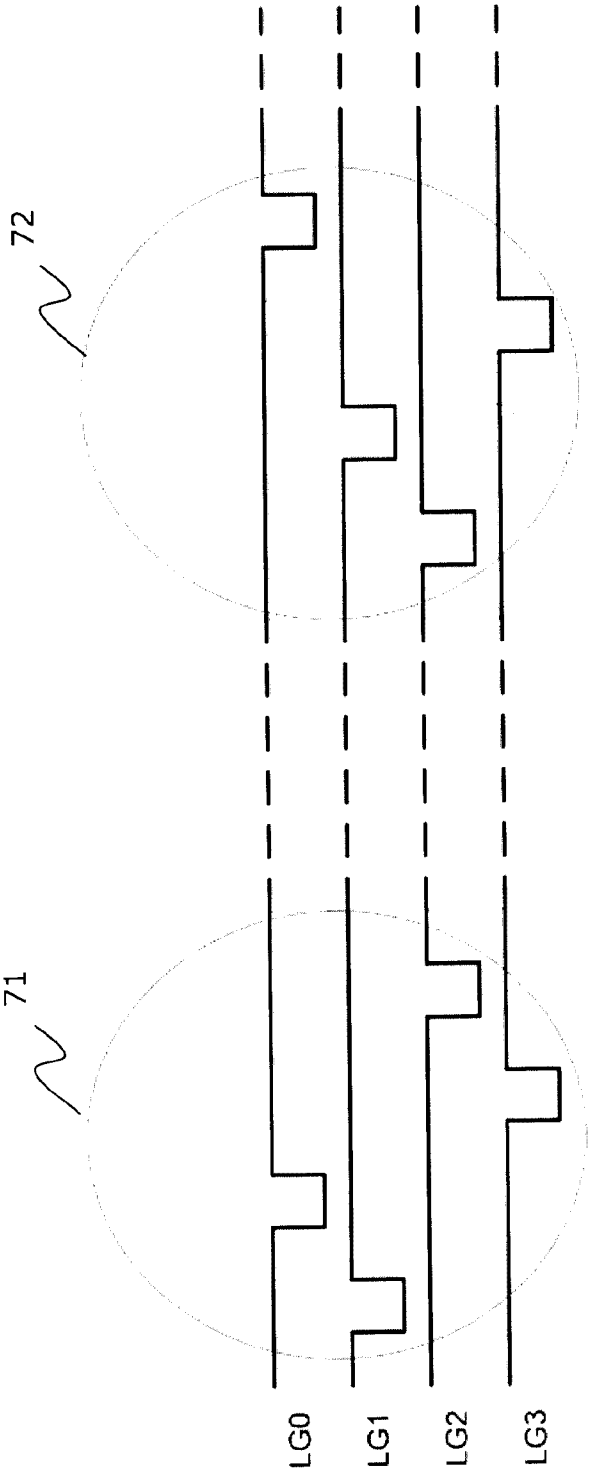


Figure 7

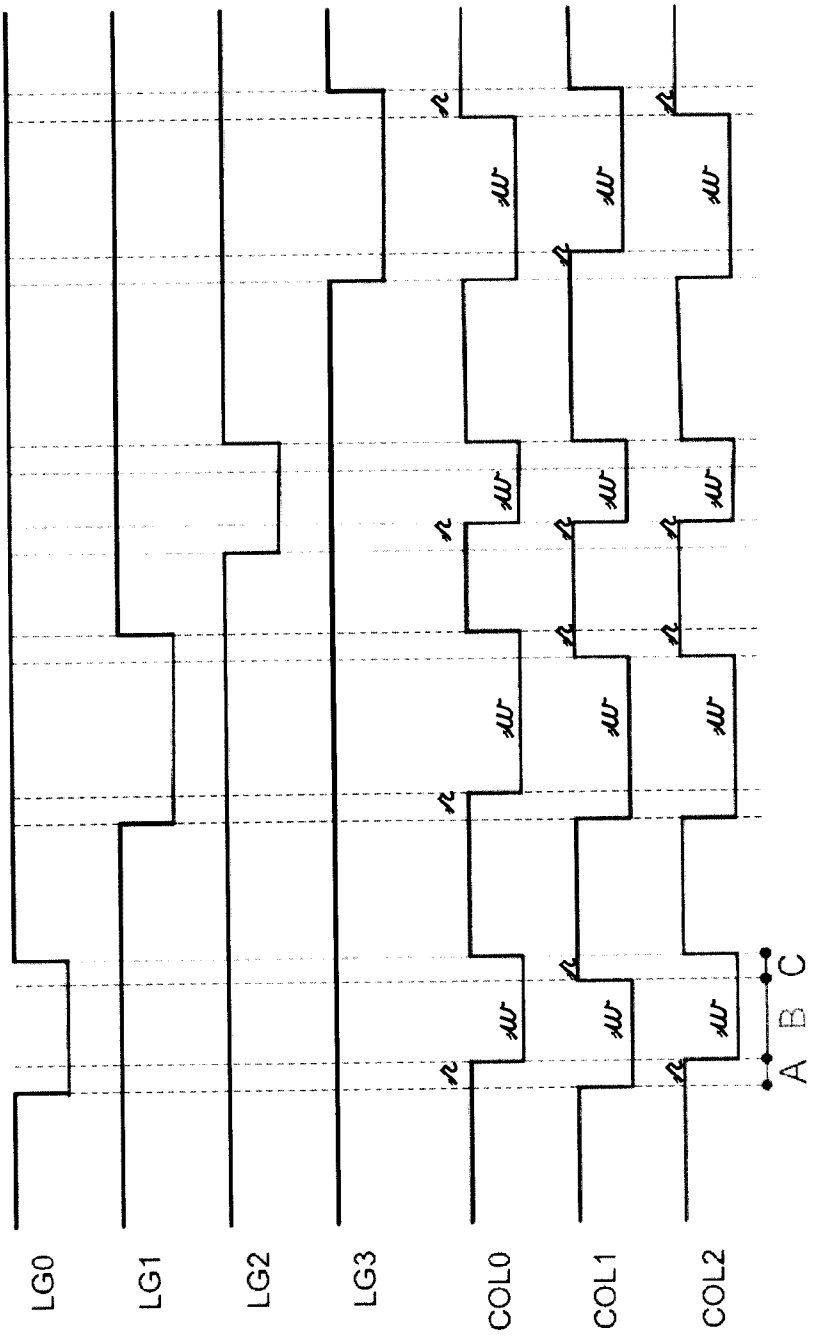


Figure 8

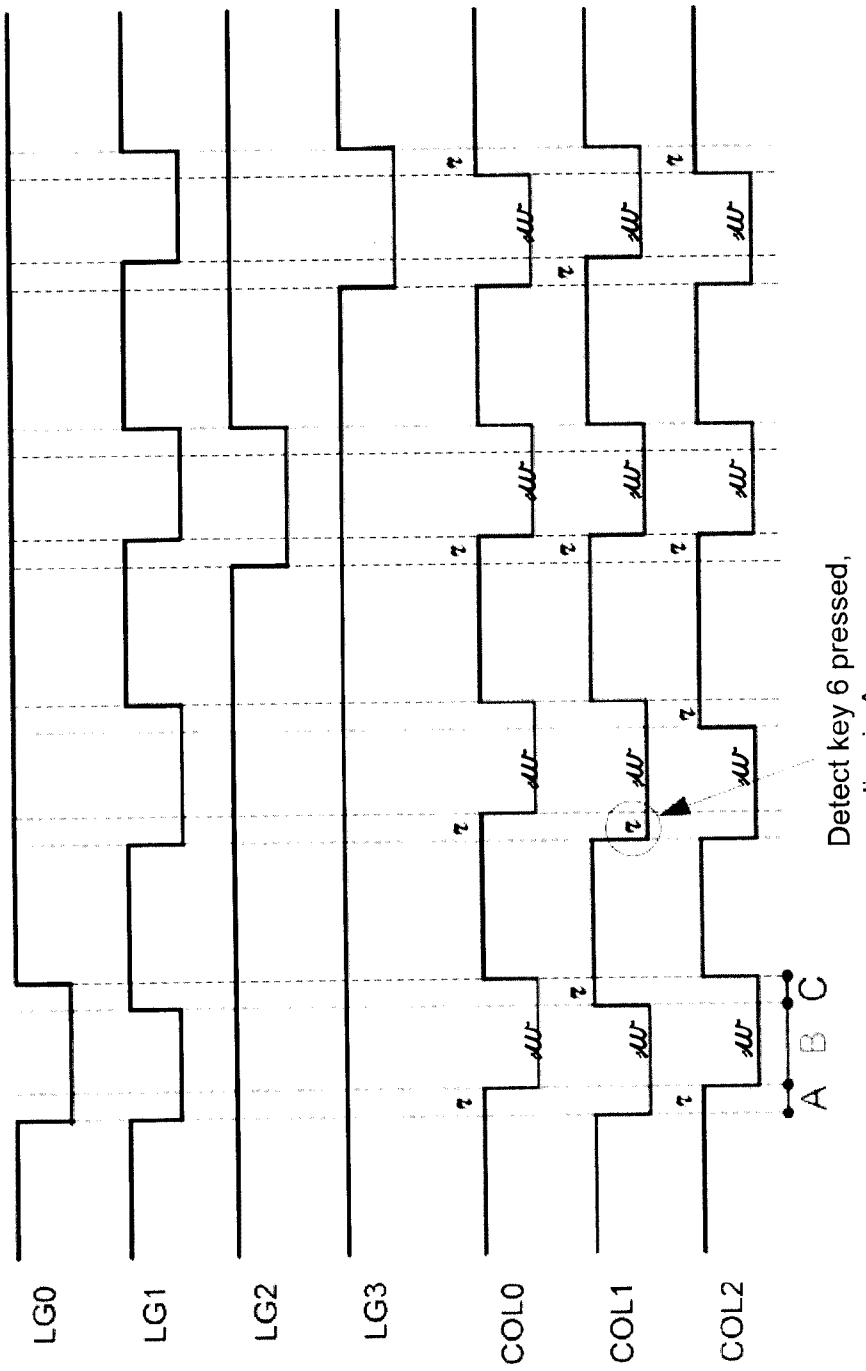

LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Detect key 6 pressed, reading in A

Figure 9

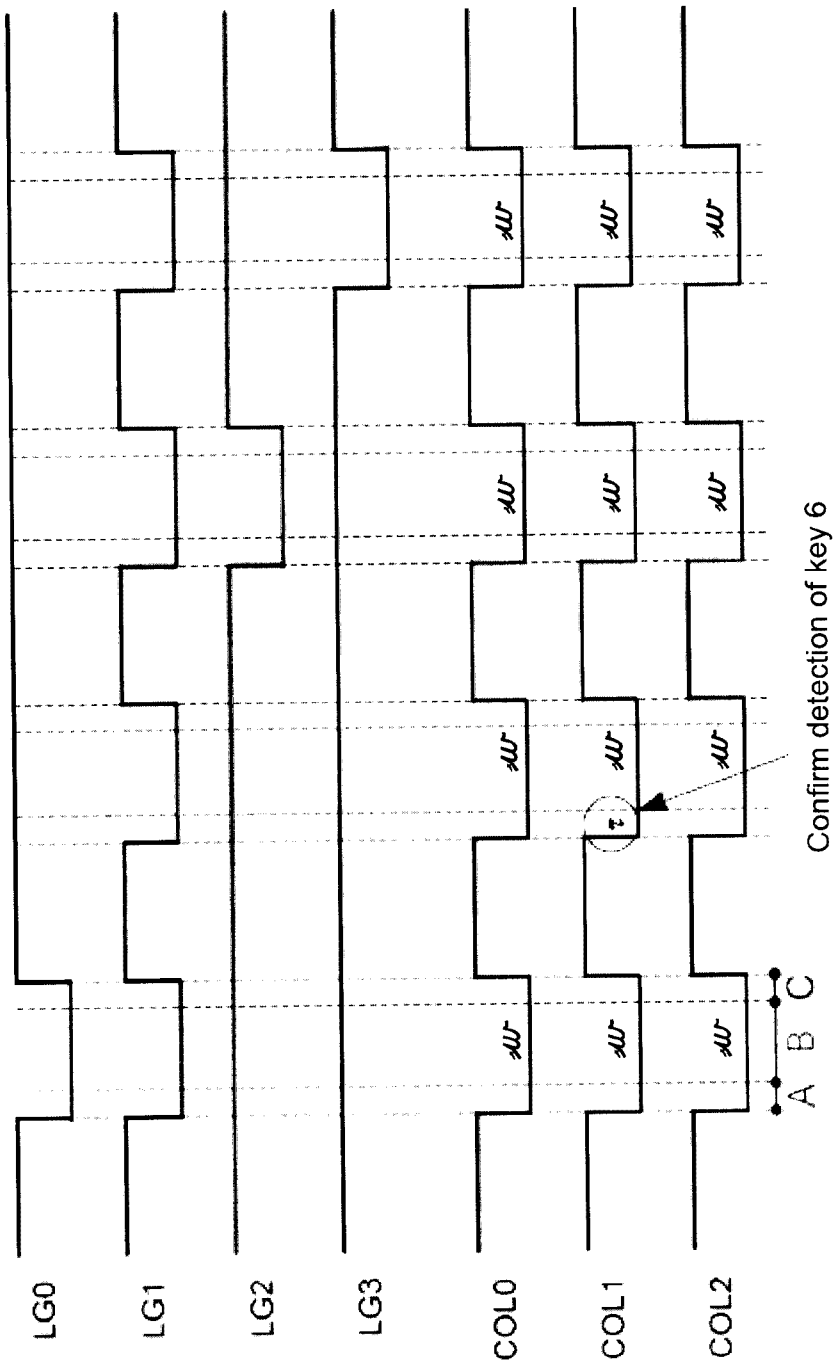

LG0
LG1
LG2
LG3
COL0
COL1
COL2
A B C
Confirm detection of key 6 pressed, reading in A

Figure 10

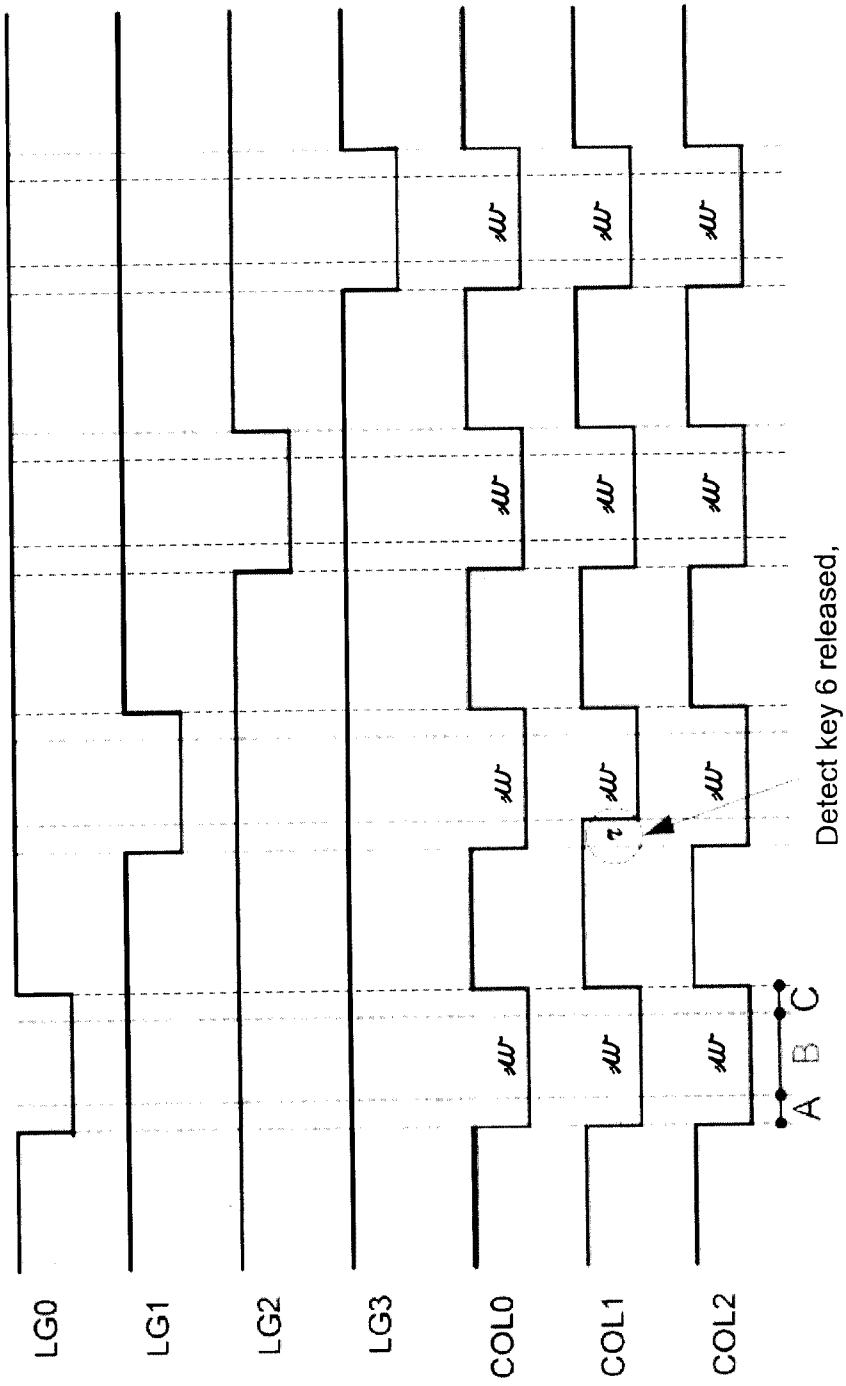

LG0
LG1
LG2
LG3
COL0
COL1
COL2
A
B
C
Detect key 6 released,
last reading in A

Figure 11

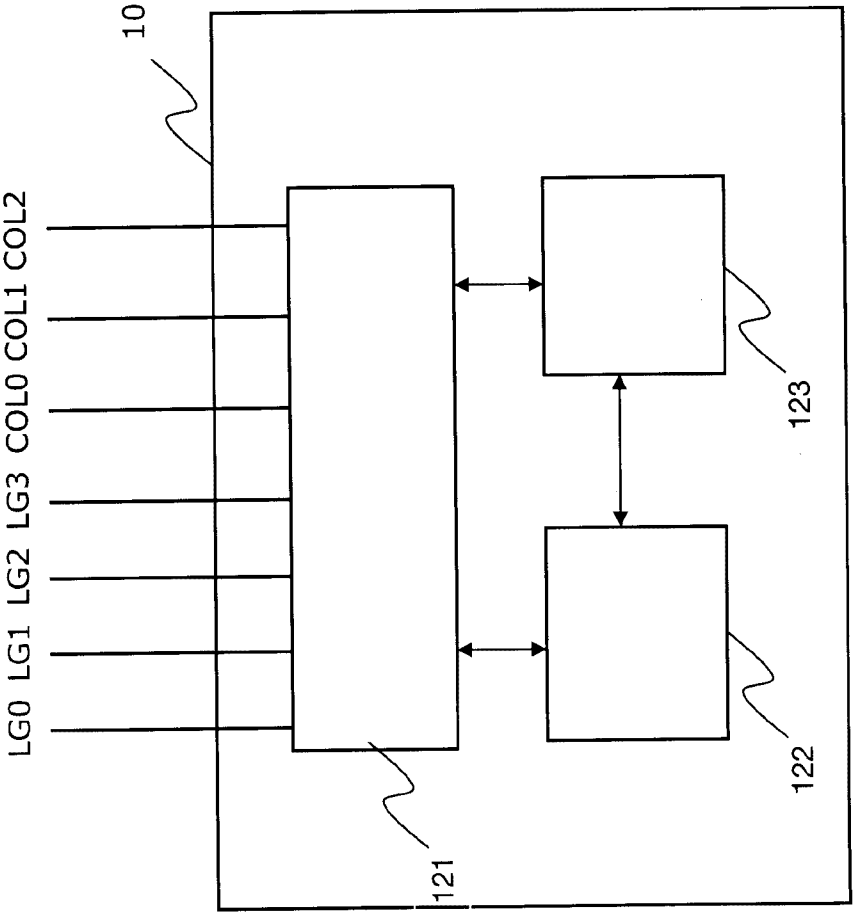
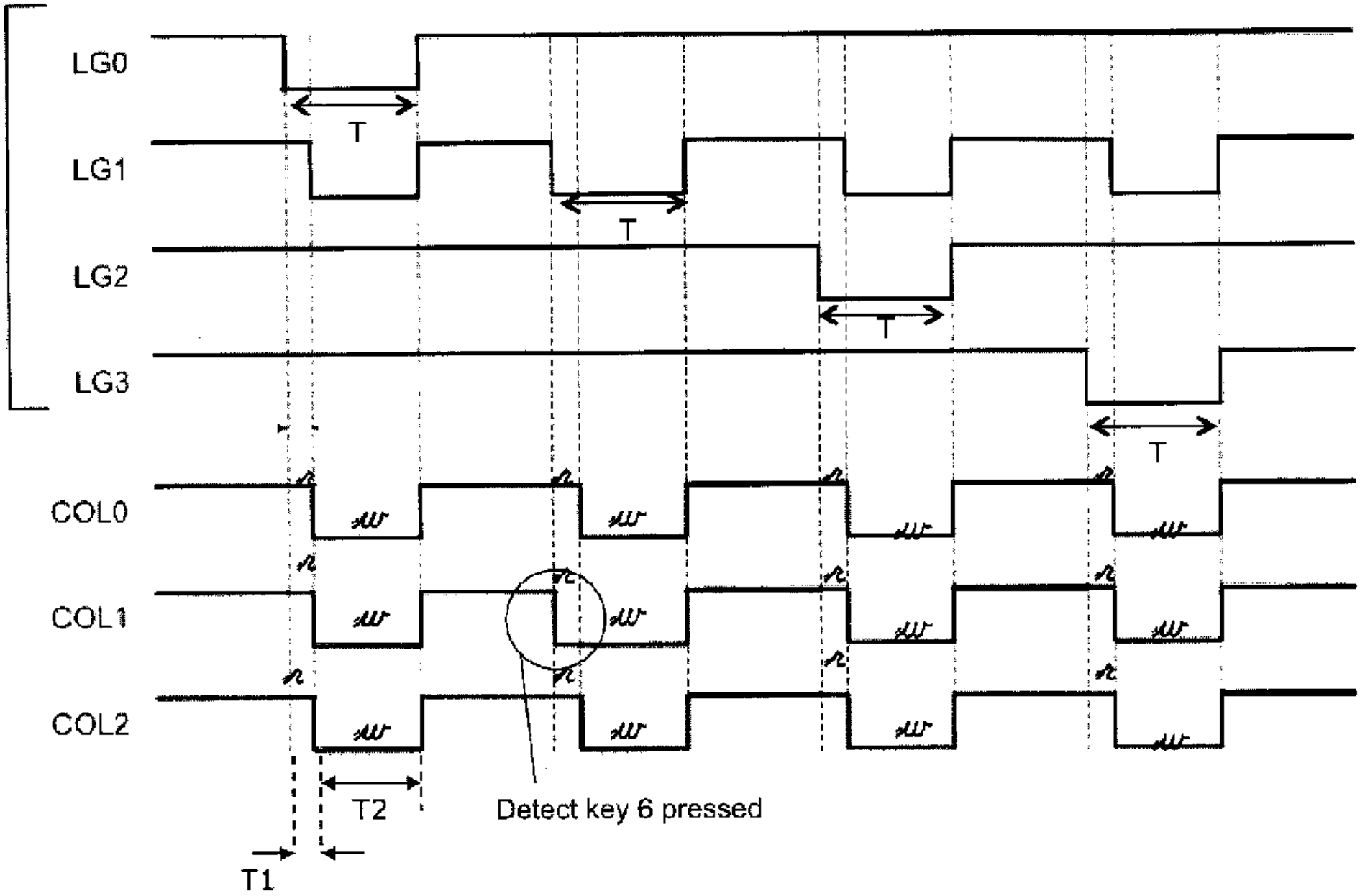


Figure 12


LG0
LG1
LG2
LG3
T
T
T
T
COL0
COL1
COL2
T2
T1
Detect key 6 pressed