Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2857504 A1 2015/01/26

(21) 2 857 504

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) **Date de dépôt/Filing Date:** 2014/07/21

(41) **Mise à la disp. pub./Open to Public Insp.:** 2015/01/26

(30) **Priorité/Priority:** 2013/07/26 (FR1357422)

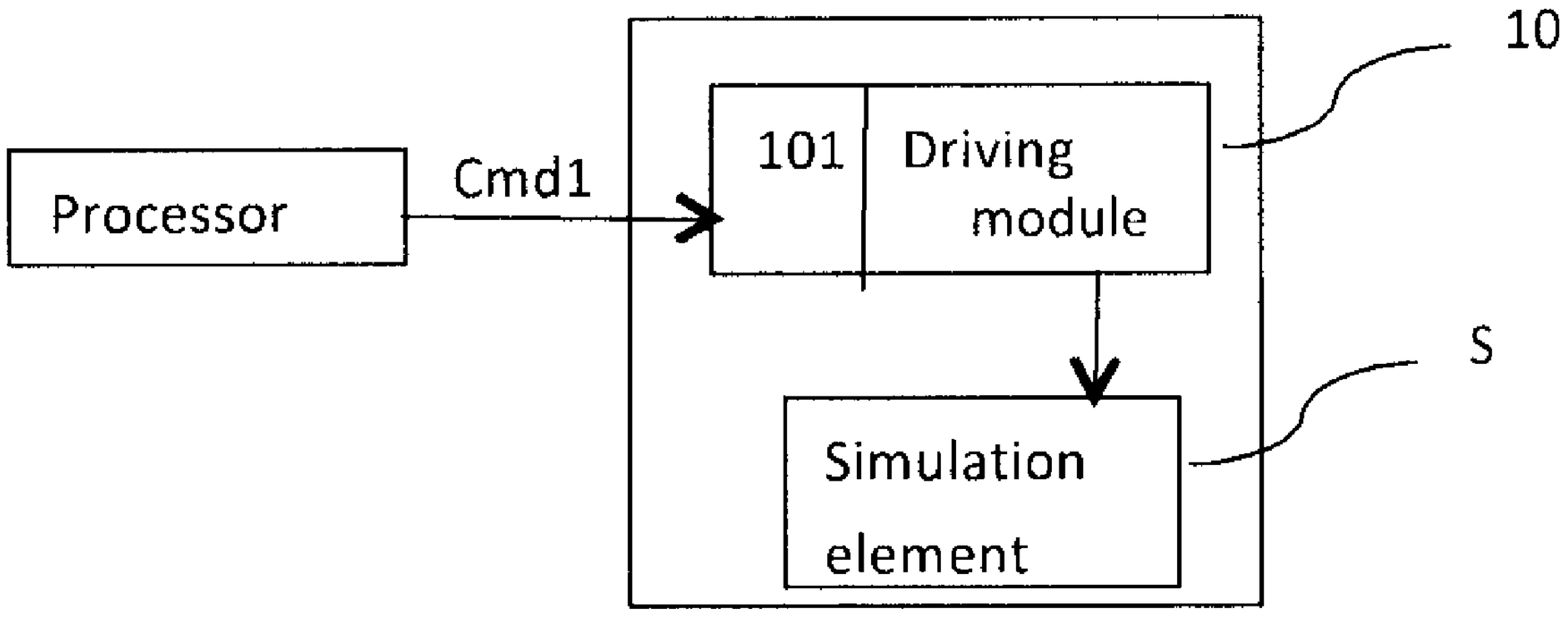
(51) **Cl.Int./Int.Cl.** ***G06F 21/83*** (2013.01), ***G06F 3/044*** (2006.01), ***H03K 17/955*** (2006.01)

(71) **Demandeur/Applicant:**
COMPAGNIE INDUSTRIELLE ET FINANCIERE D'INGENIERIE "INGENICO", FR

(72) **Inventeurs/Inventors:**
FLEURY, FABRICE, FR;
LEMAIRE, JEAN-ERIC, FR

(74) **Agent:** OYEN WIGGS GREEN & MUTALA LLP

(54) **Titre : DISPOSITIF POUR SECURISER UN CLAVIER CAPACITIF ET TERMINAL CORRESPONDANT**
(54) **Title: DEVICE FOR SECURING A CAPACITIVE KEYPAD AND CORRESPONDING TERMINAL**



(57) **Abrégé/Abstract:**
The invention pertains to a securing device for securing a capacitive keypad of an electronic payment terminal comprising at least one processor for managing the keys of said capacitive keypad.

According to the invention, such a securing device is capable of communicating with said processor and comprises a driving module (10) for driving at least one simulation element (S) for simulating at least one keystroke on said capacitive keypad, said driving module comprising reception means (101) for receiving at least one simulation command (Cmd1) randomly transmitted by said processor.

ABSTRACT

Device for Securing a Capacitive Keypad and Corresponding Terminal

The invention pertains to a securing device for securing a capacitive keypad of an electronic payment terminal comprising at least one processor for managing the keys of said capacitive keypad.

According to the invention, such a securing device is capable of communicating with said processor and comprises a driving module (10) for driving at least one simulation element (S) for simulating at least one keystroke on said capacitive keypad, said driving module comprising reception means (101) for receiving at least one simulation command (Cmd1) randomly transmitted by said processor.

Figure 1

Device for Securing a Capacitive Keypad and Corresponding Terminal

1 FIELD OF THE INVENTION

The present invention relates to the field of the securing of payment terminals, and more particularly to the protection of data entered by a user through the keypad of such terminals.

Indeed, such data, such as for example the secret code entered by the user, can be considered to be sensitive data that must be protected from possible hackers to meet the standards of safety and comfort for putting such terminals on the market.

In particular, the invention can be applied to electronic payment terminals having a capacitive keypad.

2 PRIOR-ART SOLUTIONS

Certain present-day electronic payment terminals integrate a touch pad. This raises new problems of security related to snooping on the use of such keypads.

Indeed, there exist "snooping" systems that seek to try and retrieve the data entered by a user through the touch keypad of an electronic payment terminal, for example by observation of the "traces" left by the user's fingers or again by measurement of the signal levels at the keys of a capacitive keypad. Now, there is no reliable solution to date that can overcome this problem of the hacking of a capacitive keypad.

Certain prior-art solutions are aimed at detecting the deterioration of such a keypad, for example a tearing away or a breakage of the keypad glass. This is done by adding a "guard ring" around the keypad, for example in the form of a conductive line made of copper or according to a technology known as the ITO (Indium Tin Oxide) technology.

By contrast, this type of approach for protecting touch keypads against intrusion does not resolve the problems of the hacking of data entered via capacitive keypads.

3 SUMMARY OF THE INVENTION

The invention does not have the drawbacks of the prior art. Indeed, the invention relates to a securing device for securing a capacitive keypad of an electronic

payment terminal comprising at least one processor for managing the keys of said capacitive keypad.

According to the invention, the securing device is capable of communicating with said processor and said securing device comprises a driving module (10) for driving at least one simulation element (S) for simulating at least one keystroke on said capacitive keypad, said driving module comprising reception means (101) for receiving at least one simulation command (Cmd1) randomly transmitted by said processor.

Thus, the invention proposes a novel and inventive solution to the securing of a capacitive keypad of an electronic payment terminal, especially with respect to "hackers" applying systems for snooping on the entry of a confidential code based on a measurement of the signal level of the keys for example.

The solution of the invention is based on the simulation of random keystrokes, for example during an entry of confidential data by a user, so as to disrupt any snooping operation. Besides, since this simulation is driven by the processor for managing the keys of the capacitive keypad of the electronic payment terminal itself, the working of this processor is not disrupted by these simulated keystrokes because it does not interpret the simulated keystrokes, originating from itself, as real keystrokes.

However, a snooping device applied to the capacitive keypad of the electronic payment terminal would be disrupted by these random keystrokes, which it would interpret as real keystrokes which would therefore prevent it from detecting sensitive data being entered by the user at the same time.

According to one particular characteristic of the invention, the simulation element (S) implements at least one capacitor (CP1) of a predetermined value called a parasitic capacitor and the driving module activates this parasitic capacitor (CP1) by closing at least one switch, said parasitic capacitor (CP1) being connected, when said switch is closed, to at least one receiver electrode (Y1) connected to at least one key of said capacitive keypad.

Thus, according to this embodiment of the invention, the securing device implements a simulation of a keystroke via a capacitor called a parasitic capacitor activated for example by the closing of a switch upon reception of a simulation

command coming from the processor of the electronic payment terminal. In this way, when the switch is closed, the parasitic capacitor is directly connected to a receiver electrode itself connected to one or more keys of the touch keypad.

Depending on the characteristics of the simulation command (duration, frequency, etc), one or more keys connected to the receiver electrode are involved and one or more keystrokes are therefore simulated.

According to one particular characteristic of the invention, the simulation element (S) implements at least one capacitor (CP1) of a predetermined value, called a parasitic capacitor, and the driving module activates this parasitic capacitor (CP1) by means of at least one transistor, said parasitic capacitor (CP1) being connected, when said transistor is activated, to at least one receiver electrode (Y1) connected to at least one key of said capacitive keypad.

Thus, according to this embodiment of the invention, the securing device implements a simulation of a keystroke via a capacitor called a parasitic capacitor activated for example by means of a transistor upon reception of a simulation command coming from the processor of the electronic payment terminal. In this way, when the transistor is activated, the parasitic capacitor is directly connected to a receiver electrode itself connected to one or more keys of the touch keypad.

Depending on the characteristics of the simulation command (duration, frequency, etc), one or more keys connected to the receiver electrode are concerned and one or more keystrokes are therefore simulated.

In particular, the driving module is capable of driving at least two parasitic capacitors (CP1, CP2) upon reception of at least two distinct simulation commands (Cmd1, Cmd2) coming from said processor, each of said parasitic capacitors being connected to a distinct receiver electrode (Y1, Y2) enabling the simulation of at least all the numerical keys of said capacitive keypad.

Thus, according to this embodiment of the invention, at least all the numerical keys corresponding most of the time to sensitive data such as a confidential code or a bank card number can be simulated to deceive a possible spy device implemented on the capacitive keypad of the electronic payment terminal.

For example, the predetermined value of said parasitic capacitor corresponds appreciably to a capacitive value representing a stroke on a key of said capacitive keypad.

According to one particular aspect of the invention, the device is implemented in a secure zone of said electronic payment terminal.

Thus, according to this embodiment of the invention, the securing device is itself located within the electronic payment terminal in a zone protected by means implemented in the electronic payment terminal so that the securing device cannot be inhibited or damaged. The security of the entry of sensitive data on the capacitive keypad of the electronic payment terminal is therefore optimal.

The invention also concerns an electronic payment terminal comprising a securing device as described here above.

The invention also concerns a method for securing a capacitive keypad of an electronic payment terminal comprising at least one processor for managing keys of said capacitive keypad comprising the following steps:

- a reception step (30) for receiving at least one simulation command (Cmd1) transmitted randomly by said processor;
- a driving step (31), activated by said reception step , for driving at least one simulation element (S) for simulating at least one keystroke on said capacitive keypad;
- a simulation step (32) for simulating at least one keystroke on said capacitive keypad.

The invention also pertains to a computer program downloadable from a communication network and/or stored on a computer-readable medium and/or executable by a processor comprising program code instructions to execute the method of securing as described here above when it is executed by a processor.

4 LIST OF FIGURES

Other features and advantages of the invention shall appear more clearly from the following description of a particular embodiment given by way of a simple illustratory and non-limiting example and from the appended drawings, of which:

- Figure 1 is a diagram of a device for securing a touch keypad of an electronic payment terminal according to one embodiment of the invention;
- Figures 2 and 4 present two examples of implementing a device for securing a touch keypad of an electronic payment terminal according to one embodiment of the invention;
- Figure 3 presents the main steps of the method for securing a touch keypad of an electronic payment terminal according to one embodiment of the invention.

5 DETAILED DESCRIPTION OF THE INVENTION

5.1 General principle

The principle of the invention consists of the implementation of a device for securing the capacitive keypad of an electronic payment terminal. This device, applied in the electronic payment terminal, is aimed at deceiving a system that might be snooping on the keystrokes on the keypad, for example when a user is entering sensitive data.

Indeed, the principle of the invention relies on the simulation of keystrokes so as to disrupt any snooping system based on the measurement of the signal at the keys of the capacitive keypad. Thus, this simulation can be implemented for example at the same time as the real entry of data by a user via the capacitive keypad, namely at a time when a possible snooping device is also being used.

However, with these keystroke simulations, the securing system should not disrupt the process for managing keys of the electronic payment terminal itself. This is why the invention provides that the securing device will communicate with the process for managing keys of the capacitive keypad of the electronic payment terminal. This communication can be done directly, from the processor for managing keys of the securing device according to the invention or via one or more intermediate modules/elements according to the different particular embodiments of the invention.

Thus, in its different embodiments, the invention provides that this processor will randomly transmit one or more keystroke simulation commands to the securing device in order to deceive any snooping system. As a result, since it is the processor that is the source (directly or indirectly) of the keystroke simulating commands, it is not

disrupted in its interpretation of "real" keystrokes performed by a user on the keypad. Indeed, the processor knows the time at which it transmits a keystroke simulation command and therefore does not interpret the simulated keystroke as being a real keystroke.

Finally, the random nature of this simulation of keystrokes prevents a detection of the securing device of the invention in such a way that a snooping device, if any, cannot be modified to take account of it. Thus, even if a snooping system, if any, were to suspect the existence of the implementing of this securing device according to the invention, it would not be able to avoid it since the simulated keystrokes cannot be identified or predicted because of their random nature.

It must be noted that the invention also applies to any payment terminal having a touch pad or "touchscreen" using capacitive technology, i.e. implementing sender/receiver electrodes.

5.2 Description of one embodiment of the invention

A more detailed description shall now be provided of an embodiment of a securing device for securing a capacitive keypad of an electronic payment terminal with reference to figures 1 to 4.

Figure 1 illustrates an example of such a device comprising a driving module 10 for driving an element S for simulating keystrokes.

According to this embodiment of the invention, the driving module also comprises reception means 101 for receiving simulation commands transmitted randomly by a processor (the processor for managing the keys of the capacitive keyboard or else a processor related to the latter) of the electronic payment terminal.

Thus, at reception of a simulation command Cmd1, transmitted randomly by the processor of the electronic payment terminal and received by the reception means 101 of the driving module 10, this module activates the element S for simulating a keystroke.

A snooping system, if any, for snooping on the keystrokes on the capacitive keypad of the electronic payment terminal then detects a keystroke without however being able to identify it as a simulated keystroke. The snooping is then disrupted and it is

therefore no longer possible then to identify the data really entered by the user on this capacitive keypad of the electronic payment terminal.

Ideally, the device for securing the keypad is activated only during the real entry of data by a user on this keypad. Indeed, it is not necessary (or economical in terms of optimization of the use of components of the electronic payment terminal) to simulate keystrokes throughout the time of use of the electronic payment terminal but only during phases when the keypad is being used or even only when pieces of data identified as sensitive data are likely to be entered by a user. Furthermore, if the activation of the securing device is limited to precise instants, the detection of this device is made more difficult and its action is made more efficient.

Figure 3 illustrates the main steps implemented in a securing device as presented in figure 1, namely a first step 30 for receiving a simulation command transmitted randomly by the processor of the electronic payment terminal, activating a step 31 for driving a keystroke simulation element, leading to a step 32 for simulating a keystroke.

Figure 2 for its part illustrates a first example of implementation of a securing device of a touch keypad as described here above in an electronic payment terminal.

Thus, in this particular embodiment, the capacitive keyboard is considered to be constituted by a matrix of four columns and four rows classically having numerical keys (from 0 to 9) as well as function keys such as “Confirm”, “Cancel”, “Correct”, etc.

Each of these keys is connected to a receiver electrode enabling the detection of a keystroke, these receiver electrodes being three in number in this example and being denoted Y0, Y1 and Y2.

According to this embodiment of the invention, the securing device comprises a driving module enabling the simulation of at least one keystroke for all the numerical keys likely to be used, for example for entering a confidential code. Thus, the driving module enables the simulation of a keystroke on keys connected to the receiver electrodes Y1 and Y2 of the capacitive keyboard, the receiver electrode Y0 being no longer concerned according to this particular embodiment of the invention. To this end, two simulation elements are needed, denoted as CP1 and CP2.

It must be noted that according to different embodiments of the invention, all three receiver electrodes may be involved so as to be able to simulate a keystroke on all the keys of the keypad. This would potentially require the use of three simulation elements.

In this embodiment, each simulation element implements a capacitor called a parasitic capacitor making it possible, when actuated, to simulate one or more keystrokes.

Thus, the parasitic capacitor CP1 is connected, when activated, to the receiver electrode Y1 and the parasitic capacitor CP2 is connected, when activated, to the receiver electrode Y2.

Besides, the driving module comprises two switches, Inter1 and Inter2, which are closed upon reception of a specific simulation command received from the processor, respectively denoted as Cmd1 and Cmd2. These two switches Inter1 and Inter2 enable the connection respectively of the parasitic capacitor CP1 to the receiver electrode Y1 and of the parasitic capacitor CP2 to the receiver electrode Y2.

Thus, when a simulation command Cmd1 is received by the securing device via the reception means of its driving module, the switch Inter1 connects the parasitic capacitor CP1 to the electrode Y1 thus simulating, according to the parameters of simulation command Cmd1, strokes on one or more of the keys 1, 4, 7, +, F, Ca, Cl and V.

Similarly, when a simulation command Cmd2 is received by the securing device via the reception means of its driving module, the switch Inter1 connects the parasitic capacitor CP2 to the electrode Y2 thus simulating, according to the parameters of simulation command Cmd2, strokes on one or more of the keys 2, 5, 8, 0, 3, 6, 9 and -.

In practice, it is not necessary for all the keys to be simulated. The random simulation of four numerical keys makes it possible, for example, to deceive a possible snooping device while at the same time remaining non-detectable.

According to one embodiment illustrated in figure 4, the driving module of the securing device implements one or more transistors (T1, T2) making it possible, upon reception of one or more simultaneous commands (Cmd1, Cmd2) from the processor of the electronic payment terminal, to activate one or more parasitic capacitors (CP1, CP2)

enabling them, on their own, to disrupt the operation of one or more reception electrodes (Y1, Y2) of the capacitive keypad.

Any other means that make it possible to provide a low capacitance for the simulation of a keystroke on a capacitive keypad can of course be implemented according to other particular embodiments of the invention not described here.

CLAIMS

1. Securing device for securing a capacitive keypad of an electronic payment terminal comprising at least one processor for managing the keys of said capacitive keypad, characterized in that:

- said securing device is capable of communicating with said processor,
- said securing device comprises a driving module (10) for driving at least one simulation element (S) for simulating at least one keystroke on said capacitive keypad,
- said driving module comprises reception means (101) for receiving at least one simulation command (Cmd1) randomly transmitted by said processor,
- said simulation element (S) implements at least one capacitor (CP1) of a predetermined value called a parasitic capacitor,
- said driving module activates this parasitic capacitor (CP1) by closing at least one switch, said parasitic capacitor (CP1) being connected, when said switch is closed, to at least one receiver electrode (Y1) connected to at least one key of said capacitive keypad, and
- said driving module is capable of driving at least two parasitic capacitors (CP1, CP2) upon reception of at least two distinct simulation commands (Cmd1, Cmd2) coming from said processor, each of said parasitic capacitors being connected to a distinct receiver electrode (Y1, Y2) enabling the simulation of at least all the numerical keys of said capacitive keypad.

2. Securing device according to claim 1, characterized in that said switch is a transistor.

3. Securing device according to claim 1, characterized in that said predetermined value of said parasitic capacitor corresponds appreciably to a capacitive value representing a stroke on a key of said capacitive keypad.

4. Securing device according to claim 3, characterized in that it is implemented in a secure zone of said electronic payment terminal.

5. Electronic payment terminal, characterized in that it comprises a securing device according to any one of the claims 1 to 4.

6. Method for securing a capacitive keypad of an electronic payment terminal comprising at least one processor for managing the keys of said capacitive keypad, characterized in that it comprises the following steps:

- a reception step (30) for receiving at least one simulation command (Cmd1) transmitted randomly by said processor;
- a driving step (31), activated by said reception step , for driving at least one simulation element (S) enabling the simulation of at least all the keystrokes on said capacitive keypad;
- a simulation step (32) for simulating at least one keystroke on said capacitive keypad.

7. Computer program downloadable from a communication network and/or stored on a computer-readable medium and/or executable by a processor characterized in that it comprises program code instructions to execute the method of securing according to claim 6 when it is executed by a processor.

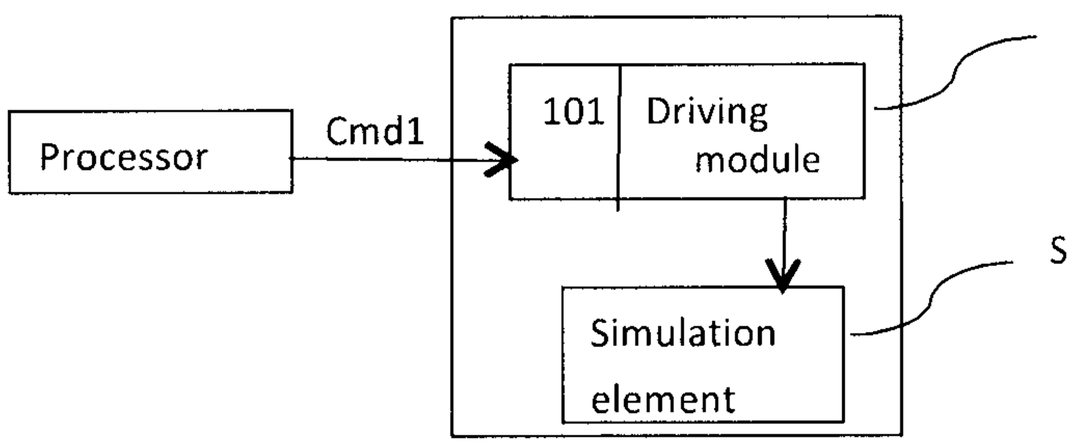


Figure 1

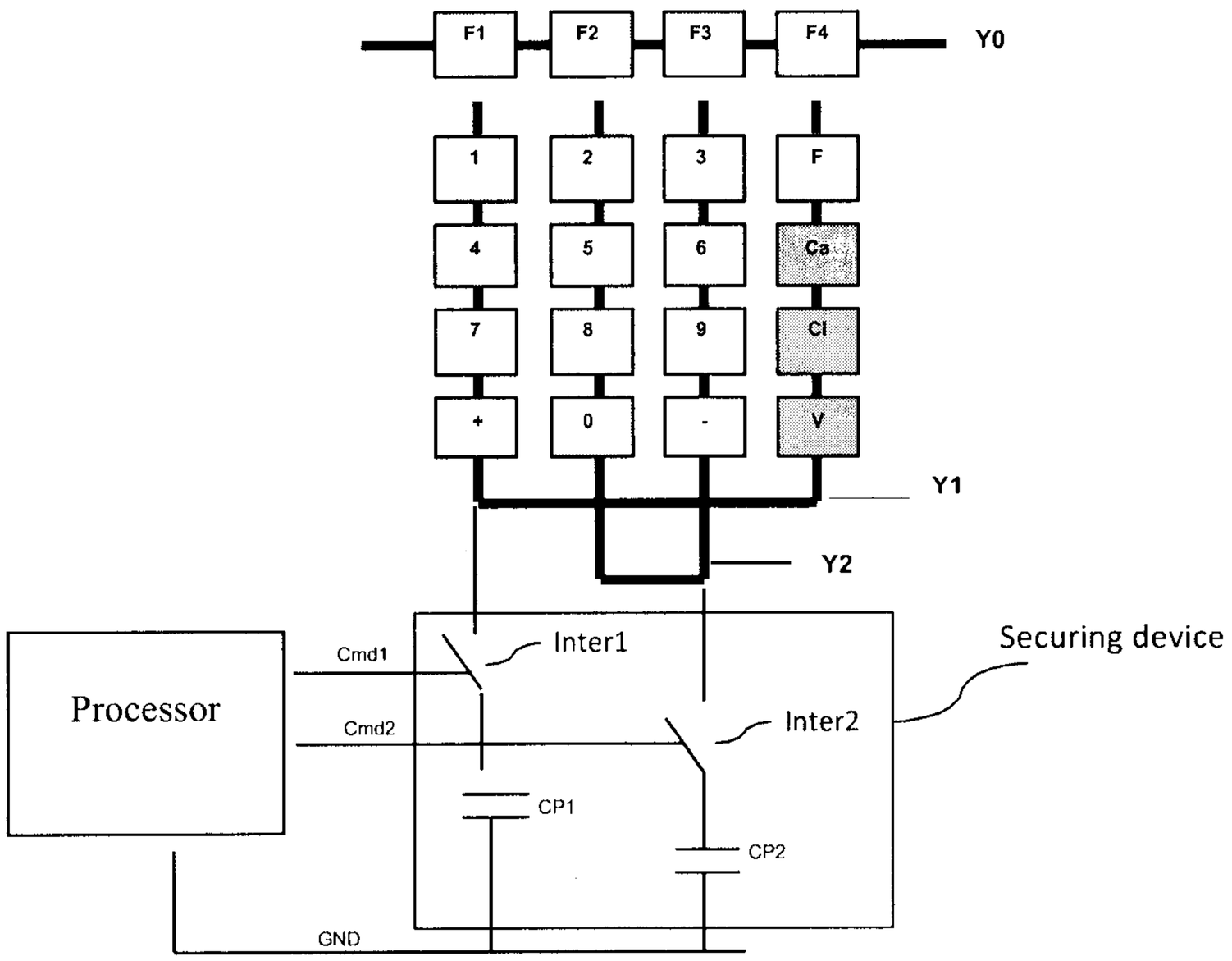


Figure 2

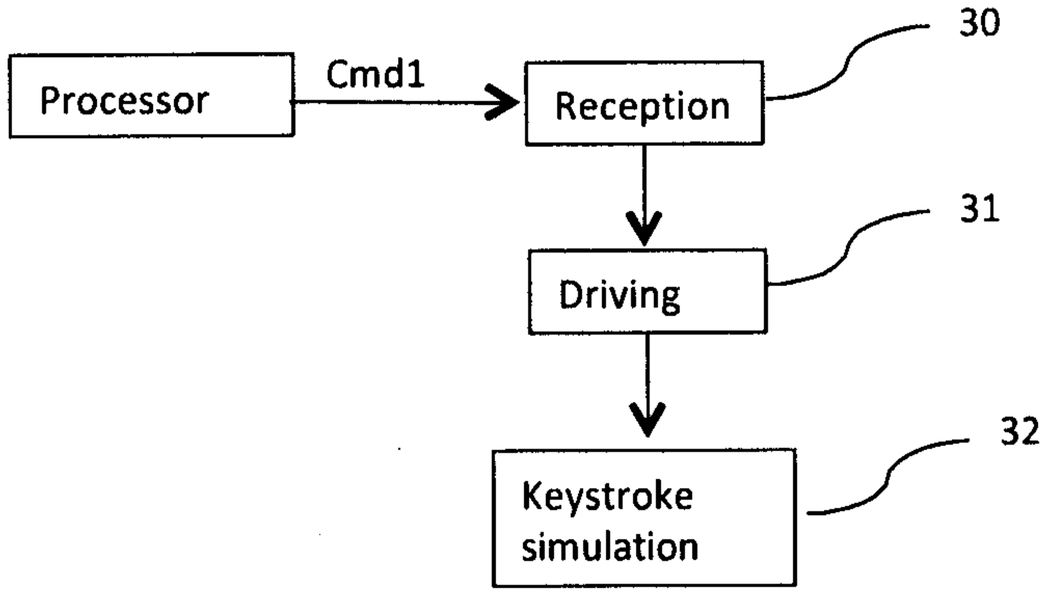


Figure 3

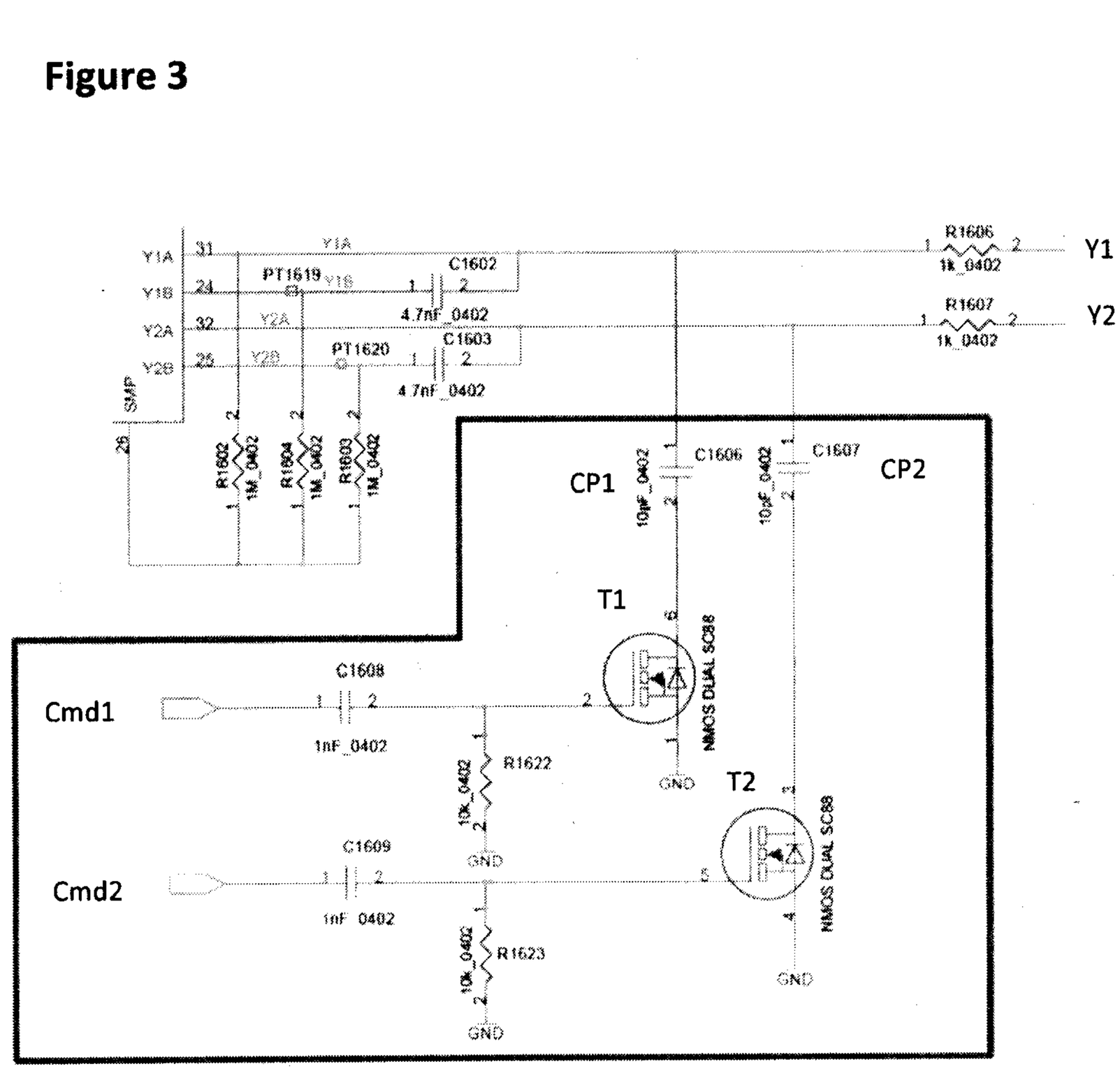
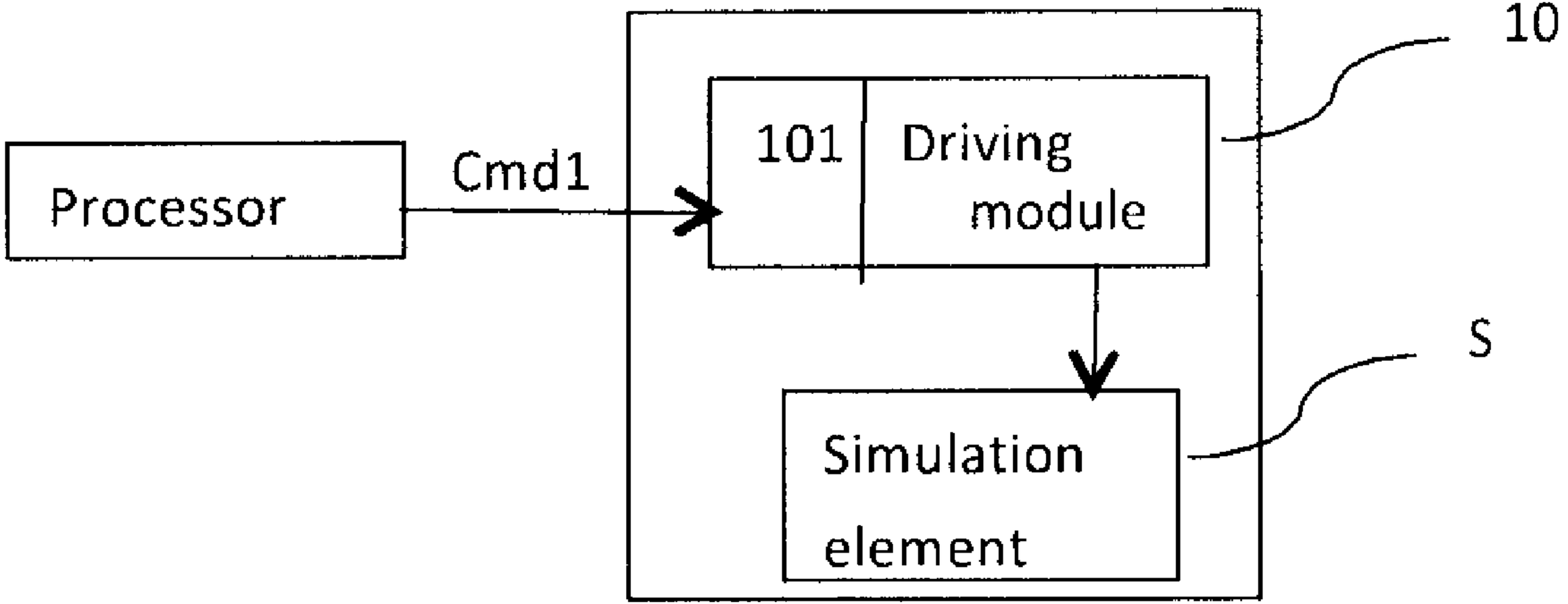


Figure 4


Processor
Cmd1
101
Driving module
10
Simulation element
S