

The present invention concerns a process for scrambling the identity of a key of a non-coded keyboard and the circuit for implementing the process.

A process is known for identifying the depressed keys of a non-coded matrix keyboard described as the line-inversion type. In this process, a universal parallel input/output interface is used in which, as shown in Figure 6, an eight-bit port is assigned to the interfacing of the keyboard by individual programming as an input or output of the lines of the port. Identification of the keys takes place in two stages.

At the first stage A, four lines of the universal port linked with the rows are programmed as an output. The four columns are programmed as an input. The value "0000" is then sent as an output to the port. This produces the value "1011" as an input. This time, the true polarities are used and the 0 corresponds to the column position where a key has been depressed, thus earthing the corresponding column.

At the second stage B the inputs and outputs are inverted. This inversion can easily be effected on a parallel interface circuit by changing the bits of the data direction register. The initial value of the data direction register was "00001111" and it has become "1111000". This operation can take place by a single instruction asking for a supplement to the content of the data direction register. The data register does not itself undergo any modifications.

The final value of the content of the data register is then read off, as can be observed in Figure 6 the input on the columns becomes "1011". The value "0" corresponds to the column on which a key has been depressed. The complete value of the data register is "1011 1011", where each 0 indicates the closing of a contact making it possible to identify currently the row and the column. The microprocessor uses this eight-bit code as a vector of connection to a table stored in an ROM which contains the eight-bit code corresponding to the key of the keyboard.

The method which has just been described has the disadvantage of making it easy for a person attempting fraud to identify the depressed key by making a connection between the wires connecting the keyboard and the interface. This is all the more of a nuisance when other measures have been taken to protect the information contained in the terminal of the device to which the keyboard is connected.

A first aim of the invention is therefore to propose a process for identifying a key of a non-coded keyboard which does not make it possible to have knowledge of the key depressed.

In the prior art, GB-A-2 190 775 describes a system in which the processor receives signals for the depression of the keys of a keyboard via specific lines during predetermined periods. Between two periods, the processor activates these lines to simulate the depression of keys on the keyboard, so that a person attempting fraud cannot distinguish between the signals representing the actual depression of a key and those simulated by the processor.

This aim is achieved by the fact that the process for scrambling the identity of a key of a non-coded keyboard, by the technique of scanning, is characterised in that it consists of:

- a) connecting as an output all the rows and columns of the keyboard to the outputs of a first register of a parallel input/output interface through the intermediary, for each output of the register, of an inverter, the output of which is connected on the one hand through a resistor to a supply voltage and, on the other hand, to the inputs with significance corresponding to a second register of the interface positioned as an input;
- b) connecting to the inputs of the second register of the input/output interface all the rows and columns of the keyboard;
- c) selecting at random the order in which the outputs will be scanned;

- d) setting at least one of the outputs to "1" and seeing whether one of the corresponding inputs is at "1";
- e) if this is not the case, scanning one by one each of the remaining lines by setting each one to "1" until the associated input is at the value "1" indicating that the line or the column has been found;
- f) repeating stages d) and e) to determine the column, or respectively, the line.

According to an additional characteristic, stage d) consists of setting two outputs of the output register (160) of the interface (16) and seeing whether one of the corresponding inputs of the input register is at 1.

According to another characteristic, the process is used to protect the information constituted by a code number entered on the keyboard (82) in a bank card reading terminal.

Another aim of the invention is to propose a circuit allowing the the process to be implemented.

This aim is achieved by the fact that this circuit comprises a circuit for a parallel input/output interface with two registers each comprising as many lines as the keyboard has lines and columns, the first register of which is positioned as an output with each of its outputs connected to an inverter, the output of which is connected on the one hand through a resistor to the supply voltage and, on the other hand, to the inputs with significance corresponding to the second register of the input/output interface positioned as an input, the rows and columns of the matrix of the keyboard each being connected to the inputs of the second register, the parallel input/output interface circuit being connected to the bus of a microprocessor to which is connected a memory containing the program for implementing the process for scrambling the identification of the depressed key.

A final aim of the invention is to propose a use of the process of the circuit to increase the security of a terminal receiving

information coming either from a microcircuit card or from a keyboard.

This aim is achieved by the fact that the process and the circuit are used to protect the information constituted by a multi-digit number entered on the keyboard in the reading terminal for a microcircuit card, the reading terminal comprising means for physically protecting the electronic circuits and the information contained in these electronic circuits.

Other characteristics and advantages of the present invention will become more clearly apparent on reading the following description, made with reference to the attached drawings, in which:

- Figure 1 shows a view of the basic diagram of the circuit for identifying the depressed key of a non-coded keyboard making it possible to implement the process of the invention;
- Figure 2 shows the stages in the process for identifying the key according to the invention;
- Figure 3 shows a diagrammatic view in section of a device for physically protecting an electronic card of a terminal;
- Figure 4 shows the diagram of the functional elements;
- Figure 5 shows the electronic diagram of the device for protecting the electronic circuit with a volatile memory in the terminal;
- Figure 6 shows the electronic circuit for identifying a depressed key for a non-coded keyboard according to the prior art.

An input/output interface (16) is connected by a bus (110) to a microprocessor (11) and a memory (13) containing, amongst other things, the management program for the input/output interface (16), and enabling the process of the invention to be implemented. The input/output interface (16) comprises a first data register (160) containing an eight-bit data byte and its associated direction register (161) which makes it possible to position this data register either as an input, or as an output. For the

requirements of the invention, the register (160) is positioned as an output. A second data register (162) receiving an eight-bit data byte as an input is also associated with its direction register (163) which positions it as an input for the operational requirements of the invention. The data received as an input by the register (162) are then transmitted to the bus (110) for processing by the processor (11) as a function of the program (130 to 157) contained in the memory (13). Similarly, the processor (11), with the aid of the program, supplies through the intermediary of the bus (110) the data to be transmitted as an output by the register (160). For each bit of the byte of the data register as an output (160) there is associated an output PA_i to which an inverter is connected. The set of eight inverters associated with the byte is represented by the reference (164). Each inverter output is connected on the one hand by a resistor to a supply voltage and, on the other hand, to the input PB_j with significance corresponding to the input register (162). The set of eight resistors associated with the inverters is represented by the reference (166).

The four most significant lines are connected to the four input lines of a non-coded keyboard, while the four least significant lines of the input register (162) are connected to the four columns of the keyboard (82). Naturally, in the description of the invention we have chosen a non-coded keyboard (82) comprising sixteen keys, and consequently having four lines and four columns, but this is not in any way restrictive and the invention can be applied whatever the dimension of the keyboards. For this, it is sufficient to find either an interface with registers of adequate dimensions, or to combine several interface circuits in parallel. The assembly of interface (16) and signal processing (11 and 13) circuits is embedded in resin, as will be seen subsequently, so as to protect them from fraudulent access. The only possible point of access for a person attempting fraud is the connector (83) which provides the link between the interface fitted in a terminal and the keyboard connected by a flexible lead to the connector.

The operation of the device will be made self-explanatory by referring to the flow chart in Figure 2. A random draw (130) first from the numbers corresponding to the columns, then from those corresponding to the lines, makes it possible to obtain the order of scanning the outputs of the register (160) which, in this example, will for example be "7, 4, 6, 5, 2, 1, 3, 0". Having made this random draw, the scanning starts for example with the lines of the matrix and to do this the stage (132) sets the outputs PA_i and PA_j with i and j comprised between 4 and 7, to the value "0". In the case of the random draw, the first outputs will be PA₇, PA₄ with the value "0". The other outputs of the register (160) being at the value "1". Thus, the word in the register (160) will be "0110111" which corresponds to the hexadecimal code "6F". At the output of the inverters (164), there will therefore be a "1" on line 7 and line 4, and "0"s everywhere else. Then, at the next stage (133), the input bit of the input register (162) corresponding to one of the two output lines which have been set to "0" is tested. If this input bit is indeed at "0" during the stage (134) the software records that the line i has been found. In the opposite case, the stage (135), the software eliminates the line i, then at the stage (136) tests the bit corresponding to the significance of the line j to determine whether its value is "0 or 1". In the case where the value is "0", the software records at the stage (137) that the line has been found and that its number is j. In the case where the value is "1", the software at the stage (138) eliminates this number j as a line number, then moves to the stage (139).

At the stage (139), another line of the output register is set to "0" and all the others to the value "1" which, in the case of the random sequence indicated above, leads us to set the line 6 to "0". The word of the output register (160) is therefore "10111111" which in hexadecimal represents the hexadecimal code "BF". Then, at the stage (141), the input line of the input register (162) having the significance corresponding to the output line, in this case PB₆, is tested and if its value is "0" the line of the keyboard in which the key has been depressed is

that corresponding to the output of the register (160) set to "0". At the stage (140), the system records that the line 2 is at "0" in the case where the key 7 has been depressed. In the case where it is not the key 7, the line PB6 is not at "0" and, consequently, at the stage (142) the number of the line is eliminated as a possible solution and the last output corresponding to a line, in this case the output PA5, is set to "0" at the stage (143). At the stage (144) the input line of the input register corresponding to the significance of the bit set to "0" is tested and, as a function of the result, it is determined whether the line is found or not. As soon as the line has been found at one of the stages (134, 137, 140 or 145), we skip to the stage (147) which sends us back to the beginning of the flow chart at the stage (132) after having forced the indices i, j, k, l to remain comprised between the values "0 and 3", so as to scan the columns. The flow chart is restarted for the values i, j, k, l comprised between 0 and 3 so as to scan the columns, and thus at the stage (132), taking account of the random draw made, PA2 and PA1 will be positioned at "0". This therefore gives us the output register "11111001", which in hexadecimal gives the value "F9".

At the stage (139), PA3 will be positioned at "0", which gives the output register the value "11110111" which, in hexadecimal, corresponds to "F7".

At the stage (143), PA0 will be given the value "0", which gives the output register the value "11111110" which, in hexadecimal, corresponds to the value "FE". In the case where it is assumed that the key 7 has been depressed, the software will determine at the stage (137) that it has found the column corresponding to the input PB1. Consequently, knowing PB6 and PB1, it will be in a position to determine that the key 7 is depressed. In the case of the key 7, the stages following the stage (136) will not be executed, and we skip direct to the stage (147) to determine the column. In the case of determining the line, we pass from the stage (140) to the stage (147). After this stage, either a loop

is made back to the input (132) of the program, or else the program is stopped if the two values have been found.

A person attempting fraud who plugs in to the connector (83) obtains the following information. When scanning the lines, at the first stage he sees the lines 1 and 4 of the matrix corresponding to the inputs PB7 and PB4 at "1", which might give him the information that it is not these lines. Then, at the next stage, he sees that the line 2 corresponding to the input PB6 is at "0" like all the others; which in this case does not give him any information. The system which has determined that the line was the second line then moves direct to scanning the columns. In view of the random draw, it starts to scan the columns 3 and 2 corresponding respectively to the inputs PB2, PB1. In this case, the person attempting fraud will read the input word "00000100" since the value "0" which is on the line PA6 at the output of the inverter will be transmitted by the matrix of the keyboard and the key 7 depressed at the input PB1, and it is this value which will prevail over the value PA1. Consequently, the person attempting fraud can only deduce from this that the column 3 is not involved. On the other hand, the system has determined for him that the key 7 was concerned. At this stage, the person attempting fraud is therefore left with an uncertainty as to the keys 5, 7, 8, 9, 11 and 12, an uncertainty which does not allow him to work out the key. As the code of a bank card is constituted of four digits, the uncertainty which is present at the level of one key becomes even more complex at the level of four digits.

If a calculation is made of the value $PF(n)$ representing the probability that the program associated with the microprocessor requires (n) stages or cycles to find the key, it will be seen that in the case of the method presented above scanning by line or column at the first cycle two lines or two columns, the following values are obtained: $PF(1) = 0$, $PF(2) = PF(3) = 4/16$, $PF(4) = 5/16$, $PF(6) = 2/16$, $PF(6) = 1/16$. Consequently, the probability of finding the key at the end of two cycles, three or four is the greatest. Even if it is found at the end of four

cycles, this leaves an uncertainty as to at least three keys for that key considered. As with the other keys of the code, it can be found in two or three cycles, the uncertainty as to the code remains sufficiently great to prevent a person attempting fraud from determining the code.

The fact that more than one output of the register is set to the value "1" is of interest from two points of view. First, this improves the probabilities and, second, it increases the difficulty for the person attempting fraud since it sometimes has two "1"s, and sometimes just one "1", or even on occasions no "1", according to whether the scanning took place with one "1" or with two "1"s. Indeed, if the above probabilities are compared with those of finding the key by applying the same method but by carrying out only one scan of an output at any one time, the following probabilities are obtained: $PF(1) = 0$, $PF(2) =$ probability of finding at the first cycle the line multiplied by the probability of finding at the first cycle the column $= 1/4 \times 1/4 = 1/16$, $PF3 = 2/16$, $PF4 = 3/16$, $PF5 = 4/16$, $PF6 = 3/16$, $PF7 = 2/16$, $PF8 = 1/16$. It may be noted therefore that if a high probability is required, it is necessary to devote between four and six cycles, which correspondingly diminishes the uncertainty for the person attempting fraud.

It is quite clear that the method is not limited to scans starting with lines. It is equally possible to start scanning the columns and thereby modifying the random draw.

This type of protection is particularly useful in the case where the keyboard is used with a protected terminal according to the embodiment in Figures 3 to 5 which we shall present below.

A card (1) comprising an assembly of electronic circuits (10, 11) is surrounded by a resistor network (2) constituted by a polycarbonate film (20), on each of the faces of which a film of carbon (21, 22) is screen printed. As can be seen in Figure 3, the tracks of carbon (22) on one face of the polycarbonate film (20)

are offset relative to the tracks (21) on the other face of the support film (20).

The assembly of these networks of carbon film (22) and (21) arranged on each of the faces respectively constituting a resistor (R1) and a second resistor (R2) which are connected to the electronic circuit of the card (1) by a connection (220) and a connection (210) respectively. The electronic card (1)/resistor network (2) assembly is embedded in the polyurethane resin. This resin remains in the solid state up to a temperature of around 100°C. The distance D between the faces of the resistor network and the printed circuit constituting the electronic card is small enough to prevent the probe of a measuring apparatus from being slid between the resistor network (2) and the electronic circuit card (1) via the faces where the card is not surrounded, since the resistor network (2) has a U-shaped cross section.

In an improved embodiment, it could be envisaged that the card could be surrounded by four resistor networks disposed such that there is no open gap to allow access to the electronic card (1).

The resin block (3) is then enclosed in a housing (4) constituted by two half moulds (40, 41), a first one of which comprises near the parting plane a magnet (50), and the second one of which (41) comprises, so as to be adjacent to the parting plane, a reed switch (51) which is connected by wires (52) to the electronic circuit of the card (1).

Figure 4 represents an interesting application of the principle of the invention according to Figure 1, particularly for protecting a credit card reader terminal. This credit card reader terminal shown in Figure 4 comprises a magnetic track reader (6) connected by an interface circuit (15) to a bus (110) to which a microprocessor (11) is connected. A second reader (5) is designed for reading credit cards comprising, in addition to the magnetic track, an integrated circuit with a self-programming microprocessor. This reader (5) is connected by a second interface (14) to the bus (110). A display device (7) constituted,

for example, by light-emitting diodes is also connected to the bus (110). A volatile random-access memory (12) is also connected to the bus (110). This random-access memory (12) (RAM) is transformed into a non-volatile memory by an accumulator (18) or a lithium battery which makes it possible to guarantee a supply to the volatile memory even in the case of a power cut in the main or auxiliary supply. This supply (18) to the RAM is transmitted by an electronic circuit (10) for detecting attempted fraud; this electronic circuit (10) is connected by the wires (220, 210 and 52) to the resistors in Figure 3 and to the reed switch (51). Similarly, a keyboard (8) is connected, through the intermediary of an interface circuit (16), to the bus (110). Finally, a programmable read-only memory, of the EPROM type, is connected to the bus (110). The terminal also comprises an interface circuit (17) making it possible to produce a connection of the type (RS232) or a local network.

The electronic circuit (10) for protecting the card (1) against fraud is shown in Figure 3. These electronics comprise a thermistor (101) fitted in a bridge constituted by resistors (1022, 1021, 1024 and 1029). The bridge is plugged in to the input of a window comparator (102) which, at its clock input (OSC), receives the signal supplied by a pulse generator constituted by the common point of a resistor (1028) and a capacitor (1022) connected in series between earth and a supply voltage. The output of the comparator (102) is sent to a first input of an AND gate (103). The second input of this AND gate (103) receives the output of a second window comparator (104), receiving at its pulse input the signal delivered by the common point of a resistor (1048) and a capacitor (1047) connected in series between the supply voltage and earth. This comparator (104) is connected to a resistance bridge constituted, on the one hand, by the resistors (21, 22) of the network surrounding the circuit and, on the other hand, by the resistors (1046, 1044 and 1049). The output of the AND gate (103) is sent to a first input of a second AND gate (105), a second input of which receives the output of an inverter (1050). This inverter (1050) has its input connected to the common point between a resistor (1051) and the reed switch

(51) connected in series between the supply voltage and earth. The output of the AND gate (105) is sent through a filter (106B) to a flip-flop (107), the clock input (CLK) of which receives the output of an oscillator (110). The output /Q of the flip-flop (107) is sent to a second filter (106A), the output of which is connected to an inverter (1080). The output of this inverter controls an electronic switch circuit (108) making it possible to cut off the output (120) supplying the volatile memories (12) of the card (1). The supply for these memories is supplied by a supply switching circuit (109) making it possible to switch automatically the supply of the terminal to a supply supplied by the lithium battery (18) connected to an input (VS) of the circuit (109).

In operation, the thermistor (101) associated with the comparator (102) makes it possible to detect whether the two temperature thresholds of -30°C and $+100^{\circ}\text{C}$ are exceeded. The -30°C threshold makes it possible to prevent the possibility, by lowering the temperature of the electronic circuit, of disconnecting the accumulator without losing the information contained in the RAMs (12). This would allow the person attempting fraud to gain access to the information contained in these RAMs (12) and constituted by the codes of customers who have used their cards. Similarly, the threshold of $+100^{\circ}\text{C}$ makes it possible to detect an attempt to melt the resin (3) with a view to gaining access to the information contained in the RAM. In both cases where one of these temperature thresholds is crossed, the circuit switches off the supply to the random-access memory (RAM), thereby causing the destruction of the information contained in the latter.

Similarly, an attempt to drill the resistor resin (21, 22) is discerned by the corresponding variation in the resistors (21, 22) detected by the comparator (104), the output of which controls the switching of the supply to the memory (12). This makes it possible to prevent the drilling of a channel for inserting a measurement probe and then tapping the information contained in the memory. Finally, the opening of the housing of the terminal being detected by the reed switch (51), the contact of which

closes when the magnet (50) is moved away from this switch. This state of affairs is detected by the inverter (1050) and transmitted by the AND gate (105) to the flip-flop (107), the output of which controls the switching of the supply to the RAM (12). The flip-flop (107) makes it possible to store one of the three detection states as soon as one of these three conditions, or two or all three conditions, occur at the same time.

In this way, a device has been produced for protecting a terminal which makes it possible to prevent attempted fraud either at the level of the keyboard, or at the level of the terminal.



CLAIMS

1. A process for scrambling the identity of the key on a non-coded keyboard (82) by the scanning technique, characterised in that it consists of:
 - a) connecting as an output all the rows and columns of the keyboard to the outputs of a first register (160) of a parallel input/output interface (16) through the intermediary, for each output of the register, of an inverter (164), the output of which is connected on the one hand through a resistor (166) to a supply voltage and, on the other hand, to the inputs with significance corresponding to a second register (162) of the interface positioned as an input;
 - b) connecting to the inputs of the second register (162) of the input/output interface all the rows and columns of the keyboard;
 - c) selecting at random the order in which the outputs will be scanned;
 - d) setting at least one of the outputs to "1" and seeing whether one of the corresponding inputs is at "1";
 - e) if this is not the case, scanning one by one each of the remaining lines by setting each one to "1" until the associated input is at the value "1" indicating that the line or the column has been found;
 - f) repeating stages d) and e) to determine the column or respectively the line corresponding to the depressed key of the keyboard.
2. A process according to Claim 1, characterised in that stage d) consists of setting two outputs of the first register (160) of the interface (16) and seeing whether one of the corresponding outputs of the second register (162) is at "1".
3. A scrambling process according to one of the preceding claims, characterised in that it is used to protect the information



constituted by a code number entered on the keyboard (82) in a bank card reading terminal.

4. A circuit (3) for implementing the process according to one of the preceding claims, characterised in that it comprises a circuit for a parallel input/output interface (16) with two registers each comprising as many bits as the keyboard has columns and lines, the first register of which (160) positioned as an output with each of its outputs connected to an inverter (164), the output of which is connected on the one hand through a resistor (166) to a supply voltage and on the other hand to the inputs with significance corresponding to the second register (162) of the input/output interface positioned as an input, all the rows and columns of the keyboard (82) each being connected to an input of the second register and an output of the first register, a microprocessor (11) connected by a bus (110) to the interface circuit (16) and a memory (13) containing the program for managing and controlling the interface (16) by the processor (11).
5. A circuit according to Claim 4, characterised in that it is used to protect the information constituted by a multi-digit number entered on the keyboard in the reading terminal for a microcircuit card, the reading terminal comprising means for physically protecting the electronic circuits and the information contained in these electronic circuits.
6. A circuit according to Claim 5, characterised in that the physical protection means are constituted by a resistor network (21, 22) embedded in resin (3) and further comprising means (104) for detecting modifications in the resistance of the network and means (101, 102) for detecting variations in the temperature of the resin.