

The subject of the present invention is an integrated circuit for memorising and confidentially processing information comprising an anti-fraud device.

5 It relates more particularly, but not exclusively, to integrated circuits of the above type known by the designation of memory cards.

Memory cards are produced with an electronic integrated circuit essentially comprising an electrically
10 programmable non-volatile memory often comprising non-modifiable confidential data, input/output means allowing the circuit to be coupled to a data-transfer device and processing means interconnected between the input-output means and the memory. In certain applications of memory
15 cards, it is imperative to protect access to certain areas of the non-volatile memory by an access key such as a confidential code associated with certain reading or writing rights in these specific areas. Numerous devices exist making it possible to dissuade fraudsters who seek
20 to discover the secret code or the access key to a memory by successive tries. Among these devices, the best known no doubt is the one which permanently memorises the key errors and blocks the operation as soon as the number of errors exceeds a predetermined value. However, this
25 device is ineffective if it is utilised on its own. In fact, when a memory cell is programmed at "1" there is a variation in the current and observation in the variation of the write current in the memory makes it possible to determine precisely the passage of a valid key on
30 condition that this current is correctly limited such that recording of the errors can not take place. In order to overcome this drawback, the technique currently used consists in programming an information item in every case, thus giving rise to a consumption of current. In
35 this case, a fraudster cannot recognise the correct tries from the incorrect tries by measuring the external current consumed by the component. The fraudster therefore cannot be informed of the results of the actions which he undertakes. This operation, although

effective, exhibits a major drawback. It necessitates a relatively large amount of memory space for recording the correct attempts which are in fact the most frequent. Now, in the case of a non-volatile memory of EPROM or similar type, it will not be possible to reuse this space. However, there is no use in keeping track of the correct attempts which are not used subsequently, in contrast to erroneous attempts which have to be used in order to block the system. Patent US 4,295,041 describes such a system.

In order to overcome this drawback, the person skilled in the art may think of programming only a single one and the same non-volatile memory cell in the case where an information item presented is correct and of programming different cells only in the case where the information item presented is incorrect. This permits a considerable gain in memory. However, an already-programmed memory cell exhibits a curve of current consumption which is different from that of a virgin memory cell. In fact, a virgin memory cell of a non-volatile memory exhibits a peak of current consumption of about 2 % at the start of programming, a peak which is practically reabsorbed after 2 milliseconds. Now, this consumption peak no longer exists when the cell is reprogrammed. It is therefore still possible for a fraudster to detect the passage of a valid key.

Finally, devices are known with fuses in which the consumption of current engendered by the fusing of the fuse is simulated. These devices are coarse given that the current consumed during fusing can have very variable excursions (Patent FR 2 311 360).

The object of the present invention is to overcome the drawbacks in the prior art while using a single point for programming of correct attempts.

The subject of the present invention is an integrated circuit for memorising and confidentially processing information such as that defined in Claim 1.

With this system, the fraudster can no longer be informed of the result of the actions which he undertakes since, whatever the results written into the first memory area or simulated in the cell, the same current
5 consumption is observed.

In the definition of the present invention, the following points will be specified for the person skilled in the art:

By information processing is understood either
10 the simple transfer of data between the integrated circuit and an external system or the transfer and the execution of a certain number of operations within the circuit itself.

By comparator is understood not only a simple
15 comparator carrying out the comparison between the authorisation data and the confidential code or access key, but also any system which, on the basis of the authorisation data or of the confidential code or access key, carries out a certain number of operations with a
20 view to authorising the continuation of the operations.

By processing means is understood all the circuits necessary for reading and writing of data in the memory as well as processing of these data. Generally, the processing means are constituted by a microprocessor
25 equipped with its attached circuits which are well known to the person skilled in the art.

According to a preferential embodiment of the present invention, when the first memory area is constituted by a non-volatile memory whose memory cells
30 are formed by floating-gate transistors, the simulation cell is constituted by a floating-gate transistor whose floating-gate is short circuited with the control gate and which exhibits the same gate-source voltage as a memory cell of the first memory area. The same gate-
35 source voltage can be obtained by applying to the control gate of the simulation cell a write control voltage equal to $\gamma \times$ the write control voltage applied to the memory cells of the first memory area, γ being the coupling

factor of a floating-gate transistor. In fact, the cell in accordance with the present invention is not a memory cell, as it does not record a bit, but a cell simulating programming at the level of the current, hence its name, simulation cell.

Other characteristics and advantages of the present invention will appear on reading the description of an embodiment given below with reference to the attached drawings in which:

- Figure 1 diagrammatically represents in the form of blocks the various parts of an integrated circuit to which the present invention can be applied,

- Figure 2 diagrammatically represents an embodiment of a memory cell of the first memory area connected to its control circuits,

- Figures 3A and 3B respectively represent a sectional view and a plan view from above of the memory cell of Figure 2,

- Figures 4A and 4B respectively represent a sectional view and a plan view from above of an embodiment of a simulation cell in accordance with the present invention, and

- Figure 5 diagrammatically represents the simulation cell of Figures 4A and 4B which is connected to control circuits.

In order to simplify the description, in the drawings the same elements bear the same references.

In Figure 1 is represented, by way of example, a memory card C, as an integrated circuit employing the present invention. It is obvious to the person skilled in the art that other integrated circuits can be envisaged for the employment of the present invention.

The memory card C represented in Figure 1 essentially comprises an electrically programmable non-volatile memory M, for example an EPROM memory, an input/output device I/O allowing the said card to be coupled to an external data-transfer device, and a microprocessor MP interconnected between the input/output

device I/O and the said memory M. In order to permit the confidential processing of certain information, the memory card contains authorisation information. These authorisation data are, in general, programmed into an area Z1 of the EPROM memory. However, for this confidential processing, the authorisation data contained in the area Z1 must in general be compared with an access key or confidential code entered from outside by the use of the input/output I/O device. Consequently, the microprocessor MP comprises means of comparison known as an identification comparator COMP intended for comparing the authorisation data contained in the area Z1 with the confidential code or access key introduced by the use of the I/O device. According to one embodiment of the prior art, this identification comparator COMP is associated with means for memorising an error bit in a first non-volatile memory area when the access key is erroneous. This first memory area is constituted, in the embodiment represented, by an area Z2 of the EPROM memory M. However, when the code introduced is not erroneous, the identification comparator sends the access bit to a second memory area which is constituted by the area Z3 of the EPROM memory M.

As mentioned in the introduction, the memorising of all the non-erroneous tries in the memory area Z3 consumes a great deal of memory space. Thus, in accordance with the present invention, the memory area Z3 can be limited to a single cell called simulation cell which, when it is activated, consumes the same current as a never-programmed memory cell of the first memory area.

In the case of electrically programmable non-volatile memories of the EPROM type in which the memory cell is constituted by a floating-gate transistor, the simulation cell in accordance with the present invention will be constituted by a floating-gate transistor whose floating gate is connected to the control gate. From a technological point of view, this simulation cell can be produced in a same memory plane as a traditional EPROM

and selected by using the same decoders and control circuits, as will be explained in more detail below.

Thus, according to one embodiment of the present invention, the first memory area Z2 intended to record the error bits is constituted by an EPROM-type memory area whose memory cells are formed by floating-gate transistors 1 such as those represented in Figures 2 and 3. Each floating-gate transistor 1 comprises two main electrodes, respectively 2 and 3, and a control gate 5 stacked on the floating gate 4. In the case of a N-channel MOS transistor, such as that represented in Figures 3A and 3B, the electrodes 2 and 3 are constituted by N⁺ diffusions in a P-type substrate. The floating gate 5 and the control gate 4 are produced for example in polycrystalline silicon while the isolation I is produced in silicon dioxide SiO₂. One of the principal electrodes, namely the electrode 2 in the embodiment represented, is connected to earth while the electrode 3 is connected via a bit line which is not represented and via an MOS transistor forming a switch 8 to a column address decoder 7. The control gate 5 is connected via another connection, called words line, which is not represented, to a line address decoder 6. The bit lines and word lines are arranged in lines and in columns in order to determine a matrix including the memory cell 1 in a way known to the person skilled in the art. In fact, the column address decoder 7 is connected to the gate of the transistor 8 one of whose principal electrodes is connected to the electrode 3 of the transistor 1 while its other principal electrode is connected via a circuit consisting of MOS transistors 11 and 12 to the biasing voltage V_{pp}. More specifically, the MOS transistor 11 is a depleted transistor one of whose electrodes is connected to the V_{pp} voltage while the other electrode is connected to one of the electrodes of the MOS transistor 12 which is an enhancement transistor. The two gates of the transistors 11 and 12 are connected in common to a programming control circuit. The other electrode of the transistor 12

is therefore connected to one of the electrodes of the MOS transistor 8 forming a switch, the mid-point between the transistors 12 and 8 being connected to a read amplifier 9.

5 In order to programme a memory cell of the type represented in Figure 2 to "1", a programming voltage equal to V_{pp} is applied to its control grid 5, by selecting the said memory cell 1 by the use of the decoders 6 and 7. In this case, the transistors 8, 11 and
10 12 correspond to a load resistor and the drain voltage V_D is equal to $V_{pp} - V_{load}$, while the gate voltage V_{gp} is equal to V_{pp} .

A simulation cell in accordance with the present invention will now be described with reference to Figures
15 4 and 5. In the embodiment represented, the simulation cell forms part of the EPROM memory field M. However, it is obvious to the person skilled in the art that this simulation cell can be produced and controlled independently, directly from the identification
20 comparator. As represented in Figures 4A and 4B, the simulation cell is constituted by a floating-gate MOS transistor 20 whose floating gate 21 has been connected to the control gate 22. In the embodiment represented, this simulation cell 20 is connected to a row address
25 decoder 6' and to the same column address decoder 7 and programming control 10 circuits as the memory cell of Figure 2. In fact, the simulation cell 20 can be connected up to the same row address decoder 6 as the memory cell of Figure 2, if it is possible to control, on
30 the decoders themselves, the signal V_{pp} and the signal V_{ref} used to obtain the same programming current. In the exemplary embodiment represented, it has been chosen, for lower consumption, to use two different row address decoders 6, 6', one receiving V_{pp} , the other receiving
35 V_{ref} , but the row selected is the same, that is to say the two decoders decode the same memory address.

In accordance with the present invention, in order to avoid fraud the simulation cell must behave,

during programming, in the same way as the memory cell 1. In order to do this, it is therefore necessary to have the same load line, that is to say the same drain-source voltage V_{ds} and the same gate-source voltage V_{gs} .

5 In the embodiment represented, $V_{ds} = V_{pp} - V_{load}$ and is identical in the two cases.

 However, $V_{gs} = \gamma V_{gp}$.

 Consequently, the same gate-source voltage in one simulation cell as in a normal cell is obtained by using
10 the factor γ . In fact, when a memory cell is programmed, the floating gate is charged and consequently, on the control gate, there is a capacitive ratio due to this charge. Thus, for example, if $V_{pp} = 22$ volts, on the control gate, there is a voltage of 22 volts $\times \gamma$ on the
15 floating gate. Also, in accordance with the present invention, in place of applying V_{pp} to the control gate/floating gate combination of the simulation cell 20, a voltage V_{ref} . will be applied which will be equal to γV_{pp} .

20 In accordance with the present invention, this voltage V_{ref} . can be obtained from the V_{pp} voltage by using a voltage subtracter circuit. This voltage subtracter circuit is constituted by the depletion MOS transistor 30, by an arrangement in cascade of five MOS
25 transistors 31, 32, 33, 34, 35, each connected as a diode, and by a depletion MOS transistor 36.

 More specifically, a first principal electrode of the transistor 30 is connected to the voltage source V_{pp} and its second principal electrode is connected at a
30 point 37 to the first electrode of the transistor 31. The gates of the transistors 30 and 31 are connected together and are connected to the point 37. The second principal electrode of the transistor 31 is connected to the first principal electrode of the transistor 32. The depletion
35 transistor 30 in fact has two roles. Its first role is to protect the transistors 31 to 36 with respect to the voltage V_{pp} as it possesses better characteristics at voltages of the order of V_{pp} , namely 20 V. Its second

role is to control the current in the chain of transistors and, consequently, the value of V_{ref} .

In the cascade arrangement of the transistors 31, 32, 33, 34 and 35, the control gates of each of these transistors are connected to their drain. Each constitutes a diode and gives rise to a calibrated potential drop V_T . However, the second electrode of the transistor 35 is connected to the first principal electrode of the depletion transistor 36 whose second principal electrode and the gate are connected to V_{ss} . A transistor 36 is therefore always conducting. It channels the current from V_{pp} towards V_{ss} and permits a better stability of the voltage V_{ref} . V_{ref} is a voltage reference and draws little current.

With the arrangement above, there is therefore obtained at the level of the point 38 the reference voltage $V_{ref} = V_{pp} - 5 V_T$, V_T being chosen such that $5V_T = \gamma$.

This circuit has been produced in a particular case for which:

$$V_{pp} = 22 \text{ V}$$

$$\gamma \approx 0.7$$

$$V_T = V_{T0} + K_B \phi_T = 1.2 \text{ V} \text{ (} K_B \text{ being the substrate effect coefficient).}$$

In the chosen technology, the transistors have a V_{T0} of 0.9V, but when their source is at a potential greater than V_{ss} , a substrate effect is added and thus a V_t of 1.2V is obtained.

It is obvious for the person skilled in the art that other circuits can be envisaged for obtaining the reference voltage such as voltage-raising circuits or pump circuits, or even more complex circuits with transistors with a special threshold voltage, with memory cells or other cells.

CLAIMS

1. Integrated circuit for memorising and confidentially processing information comprising at least:

5 - an electrically programmable non-volatile memory (M), containing, inter alia, authorisation data, input/output means (I/O) allowing the circuit to be coupled to a data-transfer device

 - processing means (MP) interconnected between the
10 input/output means and the non-volatile memory, the said processing means comprising, inter alia, an identification comparator (COMP) intended for comparing the authorisation data with a confidential code or access key introduced by use of the input/output means, the
15 identification comparator being associated with means for memorising an error bit in a first, non-volatile memory area (Z2) when the code introduced is erroneous, and a simulation cell (20) activated when the code introduced is correct, this cell consuming a current which is
20 identical to the current necessary for programming the error bit in the first memory area,

 this circuit being characterised in that the simulation cell is constituted by a floating-gate transistor whose floating gate is short circuited with
25 the control gate and which exhibits the same gate-source voltage as a floating-gate transistor constituting a memory cell of the first memory area.

2. Integrated circuit according to Claim 1, characterised in that the gate-source voltage of the
30 simulation cell is obtained by applying, to the control gate of the simulation cell, a write control voltage (Vref) equal to gamma times the write control voltage applied to the memory cells of the first memory area, gamma being the coupling factor of the floating-gate
35 transistor.

