This Sheet Has Been Replaced



ELECTRIC COMPONENT FOR MASKING EXECUTION OF INSTRUCTIONS OR DATA MANIPULATION

The present invention relates to an electronic component and to a method for masking the execution of instructions or the handling of data.

The present invention relates more particularly to electronic components used in applications in which access to services or to data is strictly controlled. Such a component has an architecture formed around a microprocessor and memories. It implements algorithms using secret data that is contained in the component and that is inaccessible from the outside. Such secret data can thus serve to validate or enable an electronic transaction such as a purchase, without said data being accessible from outside the component at any time.

However, by observing certain external parameters, such as the data interchanged with an external system, or the current consumed on the power supply terminal of the component, it is possible in some cases to retrieve information concerning the component by means of statistical processing. In particular, by observing the information flowing over the data bus (which is in

general a series bus) as a function of time, it is possible to obtain a correlation between said information and the procedure of the algorithm implemented in the component.

It may also be possible to obtain a correlation of said information with the observed current consumption as a function of time. It is then possible to deduce therefrom the value of a bit handled in an instruction. It is known that, at a given instant, the current consumed by a particular instruction varies depending on whether the value of the bit being handled is "0" or "1".

An object of the present invention is to mask the execution of instructions or the handling of data in the component, so as to make any observation of external parameters of the electronic component fruitless.

In the invention, provision is made to interrupt randomly the execution of the main program implemented by the electronic component so as to execute a secondary program. In this way, the procedure of the program changes all the time. Seen from the outside, it is no longer possible to perform statistical processing because the curves recorded are all offset randomly in time. For example, if the interchanged data is observed, the response time taken by the card to respond to any external command changes all the time, so that it is no longer possible to deduce therefrom any pertinent information.

As regards observing the consumed current, such current consumption over time is itself cut up and

diffused relative to the normal consumption curve, so that no pertinent information can be obtained from it.

Thus, as characterized, the invention provides an electronic component including at least one microprocessor and storage means for executing a main program.

According to the invention, the electronic component further includes a counter for counting a random value, said counter generating as output an end-of-counting information signal for suspending the execution of said main program for the time required for a secondary program to be executed by the microprocessor.

In an embodiment of the invention, the execution time of the secondary program is constant. In another embodiment of the invention, said execution time is variable. It may even be random.

In an improved embodiment, provision is made for the secondary program to activate current-consuming means so that they distort the current consumption curve of the component, thereby masking the executed operations and the handled data even more effectively.

The invention also provides a method of masking the execution of operations or the handling of data in an electronic component.

Other characteristics and advantages of the invention are described in more detail in the following description given by way of non-limiting example and with reference to the accompanying drawing, in which:

Figure 1 is a block diagram of a variant of an electronic component of the invention; and

Figure 2 shows a variant of the block diagram of a variant of an electronic component of the invention.

Figure 1 is a simplified block diagram of an electronic component CI of the invention. It includes a microprocessor 1 and internal resources which are connected to a data bus 6. The internal resources are constituted, in particular, by memories, and, in the example shown, by a program memory 2 and a working memory 3, by a counter 4, and by a random generator 5 for generating a random value R.

The electronic component CI includes various external connection terminals. In the example shown, it is a series data input/output component and therefore has a data input/output terminal I/O. It also has a ground terminal Vss, a power supply terminal Vcc, and terminals relating to control signals (not shown).

The microprocessor receives instructions and data via a series input/output port 8 connected to the data input/output terminal in association with an external system.

The microprocessor internally generates various control signals for managing the various internal resources.

Among these control signals, an enable signal EN for enabling the counter 4 is shown, as is a load signal LOAD for initializing the counter, and a select signal SEL for activating the random generator 5.

When it is enabled (EN activated), the counter generates an end-of-counting signal ITO. This end-of-counting information signal is used as a signal for interrupting the microprocessor. It is thus connected

to an input of the interrupt port 7 of the microprocessor. It should be noted that the expression "end-of-counting" is a general expression which means either that the counter has finished counting up to a determined value or that the counter has finished counting down to zero from a determined value.

It should be noted that, in the example more particularly shown, the counter is a hardware resource.

The microprocessor 1 executes a main program contained in the program memory and relating to data or instructions received from the series input/output port 8, in association with an external system.

In the invention, the execution of the main program is suspended at random moments, while a secondary program (contained in the program memory) is being executed.

For this purpose, at the start of the main program, a routine for initializing the counter with a new random value is provided. In practice, this routine comprises instructions for disabling the counter (EN deactivated), drawing a random value R from the random generator 5, loading (LOAD) this value in the counter, and then activating the counter (EN activated).

Once the counter has counted down to zero, it activates the end-of-counting information signal ITO, thereby causing an interruption at the microprocessor. Execution of the main program is suspended for the time necessary for the microprocessor to execute the secondary program, corresponding to the routine for managing the interruption in question.

The secondary program comprises at least the above-described sequence for initializing the counter, to a new random value, so that a new interruption can take place.

This secondary program may correspond to a fixed number of instructions. In which case, it is executed in constant time. For example, if the secondary program comprises only the instructions corresponding to drawing a new random value R from the generator 5 and to loading said new value R into the counter 4 (initialization), the secondary program can be executed in constant time.

In which case, in addition to executing the main program, pieces of code (corresponding to the secondary program) are executed in constant time at random moments.

In a variant of the invention, provision is made for the execution duration of the secondary program to be variable.

In a first practical embodiment, the second program provides a test on an item of binary data that is modified each time it goes through the program, the number of instructions executed then being a function of the result of the test. It is thus possible for the variable execution duration to depend on a mathematical function. For example, if the mathematical function requires a certain number of computation turns to reach the result, this number of turns being a function of the input data, the execution duration is variable, dependent on a mathematical function. All these techniques to reach a variable duration are well known.

In another practical embodiment, provision is made for the variable execution duration to be random. In this embodiment, provision is made for the secondary program to comprise disabling the counter, drawing a new random value, counting down to zero from said value in a count-down loop, and then initializing the counter to a new random value.

In this variant, pieces of code executed in random time at random moments are inserted into the execution of the main program.

In practice, numerous variants of the invention are possible.

In particular, in order to avoid degrading the execution time of the main program too much, it is possible to make provision to limit in time the total duration of delays due to executing the secondary program(s).

In another embodiment of the invention, provision is made not only to suspend execution of the main program at random moments, but also to make provision for additional current consumption, which "scrambles" the current consumption due to the execution of the main program.

This additional current consumption can be due instantaneously to instructions provided in the secondary program. For example, it is possible to make provision in the secondary program to execute computation turns of an algorithm, e.g. a cryptography algorithm.

This execution corresponds to an instantaneous current consumption, i.e. the execution time of the instruction, which scrambles the normal consumption of

the main program by being interposed in the normal current consumption as a function of the time due to the execution of the main program.

It is also possible to make provision for this additional current consumption to have a lasting effect for a certain length of time. The secondary program then makes provision to activate the current-consuming means, which consume current for at least a certain length of time, during the execution of the following instructions of the secondary program and of the main program.

A block diagram of an electronic component corresponding to this second embodiment of the invention is shown in Figure 2.

In addition to the above-described elements that bear the same references as in Figure 1, the electronic component includes a charge pump 9.

This charge pump is normally organized to deliver a high voltage Vpp for programming and/or erasing purposes from the power supply voltage Vcc so as to make it possible to program and/erase data in an electrically programmable and/or erasable read-only memory, such as, for example, memories commonly referred to as "EPROMs", "EEPROMs", or "flash EPROMs". In the invention, this charge pump is associated with the program memory.

In the example, it is activated by a write signal WE from the program memory.

Such a pump has the known characteristic of consuming a large amount of current during the time required to establish the high voltage at the output, and during the time required for the programming or for

the erasure, which time may be approximately a few milliseconds. By activating such a pump, e.g. by providing a programming instruction in the secondary program, high current consumption is superimposed, thereby masking the consumption of the following instructions of the secondary program and of the main program.

The invention is not limited to the above-described embodiments and variants. It covers any use of means for suspending the main program at random instants for a time that may be fixed, variable, or random, with or without means being used for adding additional current consumption.

With such masking or scrambling, by using any of the variants of the invention, or a combination thereof, no statistical processing is possible.

In practice, the choice of secondary program may depend on the application for which the electronic component is designed.

The invention applies to all components including at least one counter and a random generator. For any given electronic component, the choice of secondary program depends on the resources of the component in question, and on the effectiveness as regards the application in question.

It is also possible to use various secondary programs, which makes it possible to mix types, so as to improve the scrambling, the choice of the secondary program to be executed then being made at the beginning of the interruption routine.

Such a component is particularly well suited for use in chip cards or "smart cards", so as to improve tamper-proofing of them.

CLAIMS

1. An electronic component including at least one microprocessor (1) and storage means (2, 3) for executing a main program, said electronic component being characterized in that it further includes a counter (4) for counting a random value (R), said counter generating as output an end-of-counting information signal (ITO) for suspending the execution of said main program for the time required for a secondary program to be executed by the microprocessor.

2. An electronic component according to claim 1, characterized in that the execution time of the secondary program is constant.

3. An electronic component according to claim 1, characterized in that the execution time of the secondary program is variable.

4. An electronic component according to claim 3, characterized in that the execution time of the secondary program is random.

5. An electronic component according to any preceding claim, characterized in that it further includes current-consuming means that are activated by the secondary program.

6. An electronic component according to claim 5, characterized in that the current-consuming means comprise a charge pump (9).

7. An electronic component according to claim 5 or 6, characterized in that said means comprise instructions resulting in instantaneous consumption.

8. A method of masking the execution of operations or the handling of data in an electronic component (CI)

* C L M S *

including at least one microprocessor (1) and storage means (2, 3) for executing a main program, said method being characterized in that it consists in using a counter (4) and a random generator (5) for generating a random value (R) to suspend the execution of the main program at random instants for the time required for a secondary program to be executed.

9. A method according to claim 8, characterized in that the secondary program consists in disabling the counter (4), in drawing a new random value (R), in initializing the counter (4) with said new value, and in enabling the count-down before returning to the execution of the main program.

10. A method according to claim 8, characterized in that the secondary program can be executed in random time.

11. A method according to claim 10, characterized in that the secondary program consists in disabling the counter (4), in drawing a new random value (R), in counting down to zero from said new random value in a loop of the secondary program, then in drawing another new random value (R), in initializing the counter to said other new value, and in activating the counter, before returning to the execution of the main program.

12. A method according to any one of claims 8 to 11, characterized in that the secondary program also activates current-consuming means.

13. A method according to claim 12, characterized in that said current-consuming means comprise a charge pump (9).

14. A method according to claim 12 or 13, characterized in that said means comprise instructions causing instantaneous current consumption.

15. A method according to any one of claims 8 to 14, characterized in that it comprises various secondary programs.