

Circuit provided with a secure external access

This invention relates to a circuit provided with a secure external access.

5 The invention relates to the field of programmable integrated circuits, mainly that of circuits used for conducting confidential transactions.

Such a circuit comprises a microprocessor and, in most cases, a cache memory, a cache memory controller and/or a memory management unit. It also generally includes a non-volatile memory, one or several working memories, such as Random-Access Memory (RAM) or Read-Only Memory (ROM). It also includes, in most cases, other peripheral devices suited for the applications that it is designed to implement.

10
15

On the other hand, the circuit comprises a communication interface for external access. In other

words, this interface enables the microprocessor to exchange data with any component located outside the circuit.

5 The invention has a particularly advantageous application when this component is a memory. Indeed, it is common to attach an external memory to the integrated circuit so that the users of this circuit can avail of additional memory space.

10 It is obvious that the contents of the external memory can be accessed by the microprocessor, but they can also be accessed by any other piece of equipment. Thus, it is easy to read and even modify the data recorded in this memory. And yet, it is sometimes imperative for these contents to be protected from any
15 intervention from outside the circuit. This is mainly the case when the memories contain security-related information, such as a confidential access code or verification of a digital signature.

20 When loading a program in the external memory, it is provided that the integrated circuit that receives this program from the outside verifies its authenticity (identity of the issuing party) and its integrity (that it has not been modified by any third parties) before saving it in the memory. This verification is normally
25 carried out by means of an electronic signature protocol.

It is practically impossible to apply this protocol every time the external memory is read by the integrated circuit, since this is an operation that

requires a considerable amount of processing power and is therefore very slow.

5 The object of the present invention is therefore to increase the protection of this memory against unwanted access, while not slowing down the operation of the circuit.

According to the invention, a circuit comprises a microprocessor and a set of peripheral devices including at least one communication interface for
10 external access, wherein said peripherals, unlike the said communication interface, are connected to the said microprocessor by an interconnection bus on which the data length is equal to the standard data length of the data processed by said microprocessor. According to
15 the invention, said integrated circuit also comprises a security module connected to the said interconnection bus and to the said communication interface by a dedicated link (DL), and the length of the data processed by the security module is greater than the
20 standard data length of the data processed by the microprocessor. Therefore, the integrated circuit comprises means for adapting the length of the data processed by the security module to the standard data length. Preferably, said means for adapting the length
25 of the data processed by the security module to the standard data length include a cache memory, associated with the microprocessor and provided with a cache memory controller which, upon accessing the cache memory, causes it to transmit to the security module
30 data having a length equal to the standard data length.

The cache memory is a rapid and efficient means for preparing data to be ciphered by the security module, and also for breaking ciphered data from the format compatible with the security module, down into a format presenting a standard data length, compatible with the data bus of the microprocessor. This allows that the processing of the data by the security module is performed on the fly.

During the ciphering of the data by the security module, the cache memory prepares data having a length greater than the standard data length, whereby said data can be accepted at the input of the security module.

On the other hand, during the deciphering of the data by the security module, the cache memory breaks the deciphered data available at the output of the security module and having a length greater than the standard data length, into standard-length data.

This arrangement yields also the advantage of flexibility, since the circuit can process data of a greater or different length than the standard data length, which is particularly advantageous when the data processed by the security module are rather long, which depends on the ciphering algorithm used.

According to a preferred embodiment, the security module uses a secret key algorithm which processes data having a length of at least 64 bits, and the standard length of the data processed by the microprocessor is less than 64 bits.

The secret key algorithm is preferably the AES algorithm.

It is preferable for the encryption key to be stored in a one-time-programmable register, and this register can
5 be saved in a non-volatile memory.

The present invention will be better understood with more detail in the context of the following description of a sample embodiment provided for illustrative purposes in reference to the appended
10 figure, which shows a diagram of an integrated circuit according to the invention.

In reference to the figure, an integrated circuit IC comprises a microprocessor MIC that is possibly connected to a cache memory and/or to a memory
15 controller (not shown). It also comprises a communication interface UMI and, generally, other peripheral devices PER, such as a non-volatile flash memory, working random-access memory, etc.

According to the invention, the circuit also
20 comprises a security module CR. A system bus BUS interconnects all the elements in the circuit except the communication interface UMI, and a dedicated link DL connects this interface UMI to the security module CR.

25 Outside the circuit there is a component MEM that can communicate with the communication interface UMI, and the invention thus provides protection for the data that pass through this interface by means of the security module CR.

30 In this specific case, this component is an external memory MEM and the communication interface is preferably a universal memory interface UMI.

The security module CR can use various techniques for encoding or modifying the data it receives from the microprocessor MIC through the system bus BUS before transmitting the data thus encoded to the communication interface UMI so that they do not appear clearly in the external memory MEM. It is obvious that this module can decode the information when it reads the data in this external memory MEM in order to return them to the microprocessor MIC the same way as they were provided initially.

Thus, the data are encrypted before being saved in the external memory MEM and they are then decrypted when they are read by the said memory before being sent over the system bus BUS.

It is therefore advisable to encode the data on the fly before storing them in the external memory MEM.

The microprocessor MIC can process 8-, 16- or 32-bit data. Currently, access to external data is granted using words with a standard length of 8, 16 or 32 bits. To secure such data requires 8-, 16- or 32-bit encryption respectively. In this case the encryption would be very vulnerable, practically inefficient, if known algorithms are used.

It is therefore desirable to choose an algorithm that works with 64-bit data, or even 128-bit whenever necessary. Selecting a standard algorithm makes it possible to avoid additional constraints while guaranteeing a maximum level of security.

Algorithms with a private or secret key will be given preference since they require much less processing time than algorithms with public keys.

5 As an example, the following algorithms will be used:

- AES (Advanced Encryption Standard), working with 128-bit keys and currently providing maximum security,
- 10 - DES (Data Encryption Standard), working with 64-bit keys, known for being universally used in systems that are less demanding in terms of security,
- 3DES (Triple Data Encryption Standard), or
- 15 - XDES (Extended Data Encryption Standard), the latter two algorithms are recommended for the most demanding systems in terms of security, while ensuring high encoding rates at a low cost.

20 The security module CR makes it possible to encrypt data that are longer than the standard length. This module is designed for processing 64- or 128-bit data, recorded as eight or sixteen 8-bit words, four or eight 16-bit words, or else two or four 32-bit words respectively in the external memory MEM, therefore
25 access to any of these data is divided into several 8-, 16- or 32-bit accesses respectively.

For this purpose, the security module CR is able to process grouped or consecutive accesses of the microprocessor cache memory controller. This cache
30 memory contains a partial copy of the external memory

MEM, which is updated depending on the part of the program being run by the microprocessor MIC. Since the cache memory is very fast and very close to the microprocessor MIC, it generally allows for an
5 improvement of the circuit's performance.

The data present in the cache memory is replaced by the cache controller in packets. These packets have a minimum size of four 32-bit words, regardless of the size of the data processed by the microprocessor MIC.

10 It must be noted here that the cache memory can also be used by the circuit for other purposes.

The controller can be required to write the data saved in the cache memory that relate to the external memory MEM in packets with a size that is a multiple of
15 64 bits.

The interface between the cache memory and the external memory MEM, which can only manage 8-, 16- or 32-bit accesses is set up in a simple manner, breaking a 64-bit access down into eight 8-bit accesses, four
20 16-bit accesses or two 32-bit accesses respectively.

In the case of 32-bit access, the DES or 3DES algorithm will be loaded every two 32-bit words, while the AES algorithm will be loaded every four 32-bit words. The data are loaded on the fly. In the case of
25 "pipeline" processing of the AES algorithm, in other words when complete processing of a piece of data in one or several cycles is able to receive a new piece of data in each cycle, only the first access introduces a latency time in the total data transfer time.

The secret key used by the algorithm is preferably stored in a so-called OTP register (One Time Programmable). If the integrated circuit IC is provided with a non-volatile flash memory, this register can be
5 located there.

The example of an embodiment of the invention described above was chosen due to its concrete nature. It would not, however, be possible to exhaustively list all the possible embodiments of this invention.
10 Particularly, all the described means can be replaced with equivalent means without departing from the scope of the present invention.

CLAIMS

1) A circuit (IC) comprising a microprocessor (MIC) and a set of peripheral devices including at least one communication interface (UMI) for external access, wherein said peripherals (PER), unlike the said communication interface (UMI), are connected to the said microprocessor (MIC) by an interconnection bus (BUS) on which the data length is equal to the standard data length of the data processed by said microprocessor (MIC), said integrated circuit also comprising a security module (CR) connected to the said interconnection bus (BUS) and to the said communication interface (UMI) by a dedicated link (DL),

Wherein the length of the data processed by the security module is greater than the standard data length of the data processed by the microprocessor, and the integrated circuit (IC) comprises means for adapting the length of the data processed by the security module (CR) to the standard data length.

2) A circuit according to claim 1, wherein said means for adapting the length of the data processed by the security module (CR) to the standard data length include a cache memory, associated with the microprocessor and provided with a cache memory controller which, upon accessing the cache memory, causes it to transmit to the security module (CR) data having a length equal to the standard data length,

whereby the processing of the data by the security module is performed on the fly.

3) A circuit according to claim 2, characterised
5 in that, during the ciphering of the data by the security module (CR), the cache memory prepares data having a length greater than the standard data length, whereby said data can be accepted at the input of the security module.

10

4) A circuit according to claim 3, characterised
in that, during the deciphering of the data by the security module (CR), the cache memory breaks the deciphered data available at the output of the security
15 module and having a length greater than the standard data length, into standard-length data.

5) A circuit according to claim 4, wherein the security module (CR) uses a secret key algorithm which
20 processes data having a length of at least 64 bits, and wherein the standard length of the data processed by the microprocessor is less than 64 bits.

6) A circuit according to claim 5, wherein said
25 secret key algorithm is the AES algorithm.