



US 20070150752A1

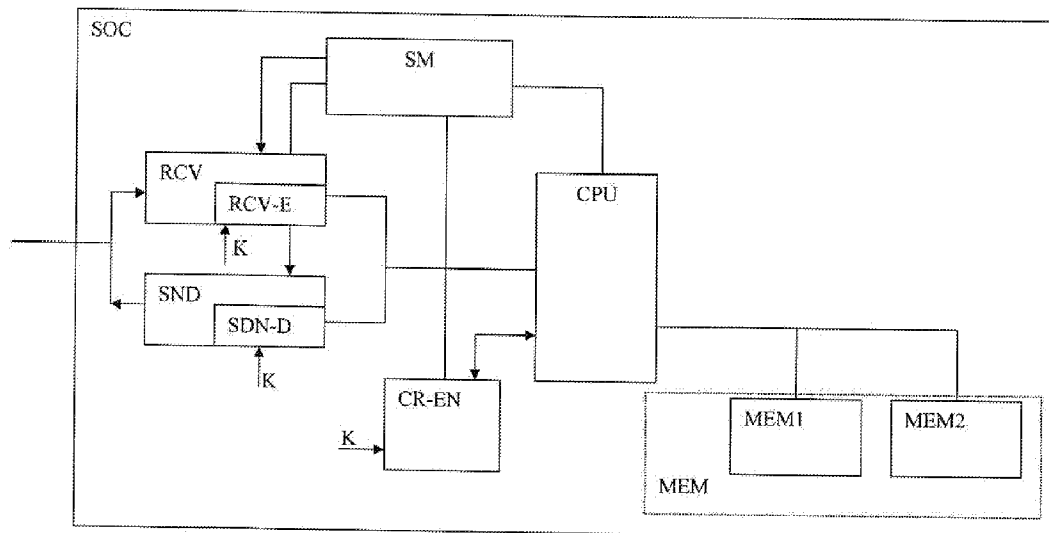
(19) **United States**(12) **Patent Application Publication**
Kudelski(10) **Pub. No.: US 2007/0150752 A1**(43) **Pub. Date: Jun. 28, 2007**(54) **SECURE SYSTEM-ON-CHIP****Publication Classification**(75) Inventor: **Andre Kudelski**, Lutry (CH)(51) **Int. Cl.**
G06F 12/14 (2006.01)(52) **U.S. Cl.** **713/190**

Correspondence Address:

DLA PIPER US LLP**ATTN: PATENT GROUP****1200 NINETEENTH STREET, NW****WASHINGTON, DC 20036 (US)**(57) **ABSTRACT**(73) Assignee: **NAGRACARD S.A.**, Cheseaux-sur-Lausanne (CH)(21) Appl. No.: **11/613,294**(22) Filed: **Dec. 20, 2006**(30) **Foreign Application Priority Data**

Dec. 23, 2005 (EP) EP 05112980.7

A secure system-on-chip for processing data comprises at least a central processing unit, an input and an output channel, an encryption/decryption engine and a memory, wherein said input channel comprises an input encryption module to encrypt all incoming data, said output channel comprises an output decryption module to decrypt all outgoing data, said central processing unit receiving the encrypted data from the input encryption module and storing them in the memory, and while processing the stored data, said central processing unit reading the stored data from the memory, requesting decryption of same in the encryption/decryption engine, processing the data and requesting encryption of the result by the encryption/decryption engine and storing the encrypted result, outputting the result to the output decryption module for decryption purposes and outputting the decrypted result via the output channel.



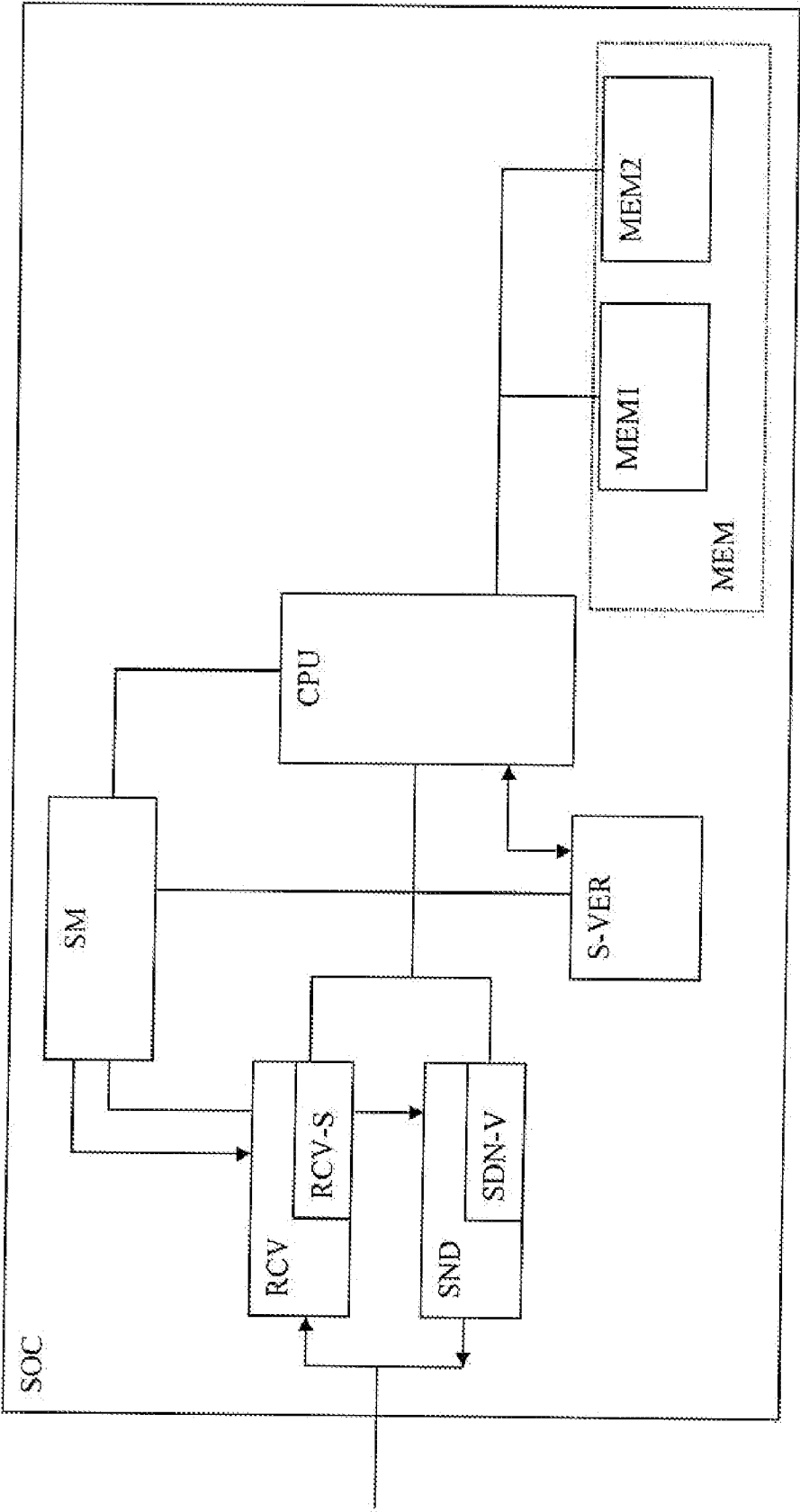


Fig. 3

SECURE SYSTEM-ON-CHIP

FIELD

[0001] The present invention concerns the field of system-on-chip and in particular the security around it.

[0002] This application is based on and claims priority to EP 05112980.7, filed Dec. 23, 2005, the entire contents of which is hereby incorporated by reference.

BACKGROUND

[0003] System-on-a-chip or System on Chip (SoC or SOC) is an idea of integrating all components of a computer or other electronic system into a single integrated circuit (chip). It may contain digital, analog, mixed-signal, and often radio-frequency functions—all on one chip. A typical application is in the area of embedded systems.

[0004] Secure environment for processors have been already disclosed, in particular with respect to multi-processing architecture. For example, a solution to limit the access to a secure memory was described in the document WO04015553. According to this solution, the processor has two modes of operations; in the first mode, called the secure mode, access is permitted to the secure memory; and in the unsecure mode, the access to the secure memory is forbidden. The unsecure mode is intended to development purposes, i.e. testing or debugging the circuit. During the execution in unsecure mode, the access to the secure memory is physically blocked, i.e. a “disable” signal is generated. This “disable” signal forbids any attempt to access the secure memory.

[0005] Another solution is described in the document PCT/EP2005/056145 in which a single chip descrambling processor processes the scrambled audio/video data in order to never leave access to the clear data. When the descrambling operation is done, the descrambling unit comprises an encryption engine to encrypt the descrambled data before they are temporarily stored in an external memory. When the processor finishes the organization task, the data are decrypted in the output module and sent to the displaying device.

BRIEF SUMMARY

[0006] The aim of the present invention is to provide a secure system-on-chip for processing data, this system-on-chip comprising at least a central processing unit, an input and an output channel, an encryption/decryption engine and a memory, characterized in that said input channel comprises an input encryption module to add an internal encryption layer on all incoming data, said output channel comprising an output decryption module to remove the internal encryption layer on all outgoing data, said central processing unit receiving the encrypted data from the input encryption module and storing them in the memory, and while processing the stored data, said central processing unit reading the stored data from the memory, requesting the removal of the internal encryption layer of same in the encryption/decryption engine, processing the data and requesting encryption of the result by the encryption/decryption engine so as to add the internal encryption layer and storing the encrypted result, outputting the result to the output decryption module for removing the internal encryption layer and outputting the result via the output channel.

[0007] The main feature of the invention is to add an encryption layer within the system-on-chip. The data entering into and exiting the system on chip are usually encrypted. An additional encryption layer is applied to these data so that all data stored in the system-on-chip have at least one encryption layer. One the data are received in the system-on-chip, they are usually decrypted with the key pertaining to the transmission system and the result is stored in clear. In the present invention, one the encrypted message is read by the system-on-chip, an internal encryption layer is applied on this message and passed to the processing unit. Said unit can store it for further use or immediately process the message. While processing the message, the first step is to remove the internal encryption layer so that the data is in the same condition as received by the system-on-chip. After the message is processed and the right (e.g.) is extracted, this right is further encrypted to add the internal encryption layer before being stored.

[0008] The removal of the internal encryption layer occurs only at the later stage when the data are really used by the central unit, the clear data being never accessible in a static state. When processed, the data can be stored in clear if they are for internal purpose or re-encrypted (i.e. adding the internal encryption layer) if they are intended to be outputted from the system-on-chip.

[0009] Once re-encrypted, the data are temporarily stored in a buffer before being sent to the output channel.

[0010] The key to encrypt and decrypt the data is in a preferred embodiment unique for that system-on-chip. This key can be preprogrammed at the manufacturing step or can be randomly generated at the initialization stage and never known by anybody. This key is used only internally. The algorithm used can be kept secret as well as the parameters of said algorithm. For example, the algorithm IdeaNxt is used as encryption engine and the values of the substitution box are randomly generated in the system-on-chip.

[0011] According to a particular embodiment, the encryption/decryption algorithm is asymmetric, so that a key pair (public/private) is used to respectively encrypt and decrypt the data.

[0012] According to an alternative embodiment, the input encryption module can be replaced by a signature module, the data being signed while entering in the system-on-chip and the signature stored together with the data. When the central unit wishes to use this data, the encryption/decryption engine which is now a signature verification engine, checks the signature and authorizes the use of the data if the signature is correct.

[0013] By data it is meant a single byte or a set of bytes e.g. to form a message or a entitlement message in the system-on-chip.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The invention will be better understood thanks to the attached figures in which:

[0015] the FIG. 1 describes the system-on-chip and its various elements in the encryption/decryption mode,

[0016] the FIGS. 2A and 2B describes the encryption stage using two units,

[0017] the FIG. 3 describes the system-on-chip and its various elements in the signature mode.

DETAILED DESCRIPTION

[0018] The secure system-on-chip SOC is based on a central processing unit CPU. The aim of this unit is to execute the code and to perform the requested tasks. The system-on-chip SOC comprises two channels connected to outer world, namely the input and the output channels. The input channel RCV comprises an input encryption module RCV-E which encrypts all the data coming from the outer world so as to add an internal encryption layer. In the same manner, the output channel SND comprises an output decryption module SND-D to decrypt the data received from the central unit CPU before sending them to the outer world so as to remove the internal encryption later.

[0019] The central unit CPU has access to the encryption/decryption engine CR-EN. This engine has the same function as the input encryption module and the output decryption module. The key K loaded in the input encryption module is the same in the encryption part of the encryption/decryption engine. The same applies to the output decryption module and the decryption part of the encryption/decryption engine, for the decryption operations. When the central unit CPU needs some data, either directly coming from the input encryption module or fetched from the memory MEM, these data are first passed through the decryption engine to remove the internal encryption layer before they are used by the central unit CPU.

[0020] In the same manner, when the central unit CPU has completed a task and produces a result, the following step being to store the result (or output the result to the output channel). This result is previously passed through the encryption engine CR-EN for adding the internal encryption layer before being stored. This encrypted result can then be stored in a memory or sent to the output channel.

[0021] The central processing unit CPU can decide if the result is to be re-encrypted or left in clear. Instead of letting the processor to decide, the target location can select different behaviors as shown in FIG. 2A. In this case, the internal encryption layer is made of two encryption units ENC1, ENC2, using two different keys K1, K2, one permanent key, and one key randomly generated. If the result is to be stored in a volatile memory V-MEM, both encryption units will encrypt the data. In the contrary if the storage is in a non-volatile memory NV-MEM (EEPROM), only one encryption unit is used, the one with the permanent key. In the same manner, when reading data from the volatile memory, the double decryption is applied although reading data from the non-volatile memory, only one decryption unit is applied.

[0022] According to an alternative embodiment shows in the FIG. 3, the encryption process is replaced by a signature process. The data are not encrypted but a signature is generated and associated with the data. For all data coming from the outer world, a signature is calculated in the input signature module RCV-S. The data are then stored with their signatures. When the central unit needs to access these data, the signature verification engine S-VER first verifies the signature before the central unit has the right to use the data. Before the data are outputted by the output channel, the

signature is verified in the output signature module SDN-V. The signature is then removed from the data which are sent to the output channel SND.

[0023] According to an alternative embodiment, the encryption/decryption engine is directly located in the central unit CPU. When a data is read from the memory, e.g. loading a variable in the accumulator of the CPU (e.g. LDAA #1200h for Motorola 68HC11), the data read at the location is passed automatically to the decryption engine so as to remove the internal encryption layer before being transferred to the accumulator. In the same manner, the instruction to store the content of the accumulator to the memory (e.g. STAA #1200h) is not directly executed but the data in the accumulator is previously passed through the encryption engine (so as to add the internal encryption layer) before being stored at the location 1200h.

[0024] In a particular embodiment, the encryption/decryption engine is shared with the input and output channel. The input encryption module is therefore a virtual module and encryption operations at the input channel are achieved by the encryption engine through a data multiplexer. The data entering into the system-on-chip SOC, in particular through the input channel are passed through the encryption engine before further manipulation e.g. to store the data in an input buffer. the input encryption module is therefore a virtual module using the resource of the encryption/decryption engine in encryption mode. The same apply for the output decryption module which uses the encryption/decryption engine in decryption mode.

[0025] The input encryption module RCV-E can comprise more than one encryption unit. According to particular embodiment shows in the FIG. 2A, two encryption units (or more) are connected in series, each having a different key. The first encryption unit is loaded with a key K1 which pertains to the system-of chip, i.e. is unique and constant for a specific device. This key is either loaded during the installation step or generated internally. The second unit ENC2 is loaded with a key K2 which is dynamically generated at the power up of the device. When the system-on-chip is reinitialized, this key is lost and a new key is generated. The data which have to be permanently stored, once processed by the processor CPU, are only re-encrypted with the first unit with the permanent key K1.

[0026] The output decryption module as well as the encryption/decryption engine comprise in the same manner also two or more units.

[0027] Alternatively, if the processor CPU recognize that the received data, stored in an input buffer, don't need to be processed but only have to be stored in a permanent memory NV-MEM, the processor can request from the encryption/decryption engine the decryption by only one decryption unit, i.e. the unit having the volatile key. The stored data still remain encrypted by the permanent key for later use.

[0028] The system-on-chip SOC can additionally comprise an autonomous supervision module SM that can deterministically control the system-on-chip SOC. This module SM, comprises a normal working condition definitions of the system-on-chip SOC, and disabling means when the normal conditions are no longer fulfilled. This is achieved by different means. A first means includes measuring the quantity of data outputted, e.g. counting the number of data sets

outputted. This operation will be hereafter described as counting data. A second means includes defining time windows during which input or output operations are allowed. A block of data is therefore allowed if the length of same do not exceed the maximum time defined for a block. A third means includes detecting the state of the central unit CPU and their respective duration, and acting accordingly as will be illustrated hereafter. The central unit CPU typically has different possible states, such as acquisition state, processing state, waiting state and outputting result state. When a message arrives to the system-on-chip, the same switches from waiting state to acquisition state. During the acquisition state, the input channel is enabled by the supervision module SM. Also during the same acquisition state, the supervision module SM counts the data arriving and compares this number to a predefined maximum. Any abnormal situation leads to a warning state in which the central unit CPU can decide how to react. The supervision module SM has the capability, especially in case of a warning state, to block the input and output channels and/or the encryption/decryption engine CR-EN.

[0029] When the external message is received, the supervision module SM causes the central unit CPU to go to processing state. During this state, the input and output channels are disabled. The supervision module SM comprises a time pattern corresponding to the minimum processing time by the central unit CPU, and disables the channels during this time. The central unit CPU can inform the supervision module SM that no result will be outputted. This has the consequence that the supervision module SM only enables the input channel for waiting a new message. The output channel then remains disabled.

[0030] In a case where the central unit CPU wishes to send data to the external world, it then informs accordingly the supervision module SM, which in turn enables the output channel. The supervision module SM still continues to watch the activities on the output channel by counting the data sent and applying a time window during which the sending is authorized.

[0031] In this embodiment of the invention, the supervision module SM is thus able to work with information received from the central unit CPU, as well as with preprogrammed working patterns.

[0032] This module can also watch the encryption/decryption engine CR-EN by counting the data encrypted or decrypted. In the same manner, the working pattern of the encryption/decryption engine CR-EN is supervised in term of data quantity processed and time. The supervision module can disable the encryption/decryption engine CR-EN if abnormal conditions are detected.

[0033] It is to be noted that the supervision module SM can be implemented in a system-on-chip without the encryption/decryption in the input/output channel. The data are processed without adding an additional encryption (or decryption) level and the input/output channel is watched by the supervision module SM.

[0034] This System-on-chip SOC is used in secure access control module in charge of receiving management messages including rights or keys. This module can also comprises an high speed descrambling unit to receive an encrypted video data stream.

What is claimed is:

1. A secure system-on-chip for processing data, the system-on-chip comprising,

- at least one central processing unit;
- an input channel;
- an output channel;
- an encryption/decryption engine; and
- a memory;

wherein said input channel comprises an input encryption module to add an internal encryption layer on all incoming data, said output channel comprising an output decryption module to remove the internal encryption layer on all outgoing data, said central processing unit receiving the encrypted data from the input encryption module and storing them in the memory, and while processing the stored data, said central processing unit reading the stored data from the memory, requesting the removal of the internal encryption layer of same in the encryption/decryption engine, processing the data and requesting encryption of the result by the encryption/decryption engine so as to add the internal encryption layer and storing the encrypted result, outputting the result to the output decryption module for removing the internal encryption layer and outputting the result via the output channel.

2. The secure system-on-chip according to claim 1, wherein the input encryption module is a virtual module which pass the data to be encrypted to the encryption/decryption engine while adding the internal encryption layer.

3. The secure system-on-chip according to claim 1, wherein the input encryption module is a virtual module which pass the data to decrypted to the encryption/decryption engine while removing the internal encryption layer.

4. The secure system-on-chip according to claim 1, wherein the algorithm to encrypt and decrypt the data is a symmetrical algorithm.

5. The secure system-on-chip according to claim 4, wherein the encryption/decryption algorithm uses a set of initialization constants and all or part of the initialization constants are randomly generated within the system-on-chip.

6. The secure system-on-chip according to claim 1, wherein the algorithm to encrypt and decrypt the data is an asymmetrical algorithm.

7. The secure system-on-chip according to claim 1, wherein it comprises means to generate randomly the key or key pair used by the encryption/decryption engine.

8. The secure system-on-chip according to claim 1, wherein the input encryption module as well as the output decryption module comprises several encryption or decryption units respectively, at least one of these units being loaded with a key which is non-volatile and at least one of these units being loaded with a permanent key.

9. The secure system-on-chip according to claim 1, further comprising an autonomous supervision module which is preprogrammed with normal working conditions definitions of at least the input and/or output data flow, and means to disable the input and/or output channel if the current conditions exceed the normal conditions definitions.

10. The secure system-on-chip according to claim 9, wherein the normal working conditions definition comprises a duration in which the supervision module comprises means to define a time window during which the input or out channel is allowed to receive or send data.

11. The secure system-on-chip according to claim 9, wherein the normal working conditions definition comprises a duration in which the supervision module disables the input and/or output channel after the reception of a block of data.

12. The secure system-on-chip according to claim 9, wherein the supervision module comprises means to receive the state condition of the central processing unit, and means to enable or disable the output channel according to the central processing unit state.

13. The secure system-on-chip according to claim 1, wherein the encryption/decryption operations can be executed on one single data or a set of data at a time.

* * * * *