(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 889 813 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
06.10.2021 Bulletin 2021/40

(21) Application number: **20217643.4**

(22) Date of filing: **29.12.2020**

(51) Int Cl.:
G06F 21/57 $^{(2013.01)}$ *G06F 8/61* $^{(2018.01)}$
H04L 9/08 $^{(2006.01)}$

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **30.03.2020 TW 109110834**

(71) Applicant: **Eco-Luxury Technology Co., Ltd.**
Zhubei City, Hsinchu County 302 (TW)

(72) Inventors:
- **LAI, YU-CHENG**
  Zhubei City, Hsinchu County 302 (TW)
- **LU, CHIA-YEN**
  Zhubei City, Hsinchu County 302 (TW)

(74) Representative: **Bandpay & Greuter**
30, rue Notre-Dame des Victoires
75002 Paris (FR)

(54) PROTECTION SYSTEM AND PROTECTION METHOD FOR SOFTWARE AND FIRMWARE OR INFORMATION

(57) A protection system and a protection method for software and firmware or information capable of encrypting and adding software and firmware or information to an electronic component, so that the software and firmware or the information is protected during the process of adding to the electronic component at a manufacturing end. Even if the encrypted software and firmware or information is obtained, the original content thereof cannot be acquired. When the electronic component is activated and used, the software and firmware or the information stored therein is then decrypted. In this way, the software and firmware or the information in the electronic component can be protected from being stolen, and the cost of the electronic component can be reduced and is easy to promote.

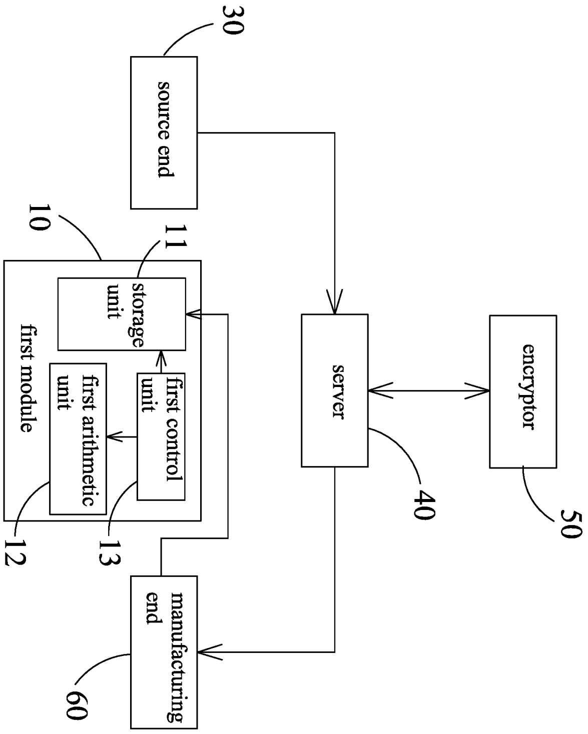

FIG. 1

EP 3 889 813 A1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

Field of Invention

[0001] The present invention relates to the technical field of software and firmware or information protection, and more particularly to a protection system and a protection method for software and firmware or information capable of encrypting and adding software and firmware or information to an electronic component and decrypting the software and firmware or the information when the electronic component is used.

Related Art

[0002] In order to execute data operating and processing in an electronic device, a large number of integrated circuit chips need to be installed. Commercial integrated circuit chips can be roughly divided into two types, one is a chip without protection function, and the other is a chip with software or firmware protection function. Chips without protection function have poor security, and internal firmware or software can be easily stolen, resulting in the leakage of business secrets. Costs of chips with protection function are relatively higher and not easy to promote.

SUMMARY OF THE INVENTION

[0003] In view of this, an object of the present invention is to provide a protection system and a protection method for software and firmware or information capable of encrypting and adding software and firmware or information to an electronic component, so that the software and firmware or the information is protected during the process of adding to the electronic component at a manufacturing end. Even if the encrypted software and firmware or information is obtained, the original content thereof cannot be acquired. When the electronic component is activated and used, the software and firmware or the information stored therein is then decrypted. In this way, the software and firmware or the information in the electronic component can be protected from being stolen, and the cost of the electronic component can be reduced and is easy to promote.

[0004] The protection system for software and firmware or information of the present invention includes a first module and a second module. The second module can have arithmetic capability or does not have arithmetic capability. The firmware or the information is encrypted with an information key by an encryptor, and then the encryptor generates a transfer key with the encrypted firmware or information by using a computation program, and encrypts the information key with the transfer key.

[0005] For the second module with arithmetic capability, the computation program is sent to the second module, the encrypted firmware or information and the encrypted information key are added to the first module, when the first module is activated, the encrypted firmware or information and the encrypted information key are sent to the second module, the second module decrypts the encrypted information key with the computation program, and then decrypts the encrypted firmware or information with the decrypted information key, and sends the decrypted firmware or information back to the first module for use by the first module.

[0006] For the second module with no arithmetic capability, the encrypted firmware or information, the encrypted information key and the computation program are added to the first module, the first module decrypts the encrypted information key with the computation program, and then sends the information key and the encrypted firmware or information to the second module. The second module decrypts the encrypted firmware or information with the information key, and the second module sends the decrypted firmware or information back to the first module for use by the first module.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007]

FIG. 1 is a block diagram of one embodiment of a protection system for software and firmware or information of the present invention encrypting software and firmware or information;

FIG. 2 is a block diagram of one embodiment of the protection system for software and firmware or information of the present invention decrypting software and firmware or information;

FIG. 3 is a schematic diagram of one embodiment of a protection method for software and firmware or information of the present invention encrypting software and firmware or information;

FIG. 4 is a schematic diagram of one embodiment of the protection method for software and firmware or information of the present invention decrypting software and firmware or information;

FIG. 5 is a flowchart of the protection method for software and firmware or information of FIG. 3 encrypting software and firmware or information;

FIG. 6 is a flowchart of the protection method for software and firmware or information of FIG. 4 decrypting software and firmware or information;

FIG. 7 is a block diagram of another embodiment of the protection system for software and firmware or information of the present invention encrypting software and firmware or information;

FIG. 8 is a block diagram of another embodiment of the protection system for software and firmware or information of the present invention decrypting software and firmware or information;

FIG. 9 is a schematic diagram of another embodiment of the protection method for software and firmware or information of the present invention encrypting software and firmware or information;

FIG. 10 is a schematic diagram of the protection method for software and firmware or information of the present invention sending a transfer key computation program to a fourth module;

FIG. 11 is a schematic diagram of another embodiment of the protection method for software and firmware or information of the present invention decrypting software and firmware or information;

FIG. 12 is a flowchart of the protection method for software and firmware or information of FIG. 9 encrypting software and firmware or information;

FIG. 13 is a flowchart of the protection method for software and firmware or information of FIG. 10 sending the transfer key computation program to the fourth module; and

FIG. 14 is a flowchart of the protection method for software and firmware or information of FIG. 11 decrypting software and firmware or information.

DETAILED DESCRIPTION OF THE INVENTION

[0008] Please refer to FIG. 1 and FIG. 2 for one embodiment of a protection system for software and firmware or information of the present invention. A protection system for software and firmware or information 100 of this embodiment includes a first module 10 and a second module 20. The first module 10 includes a first storage unit 11, a first arithmetic unit 12, and a first control unit 13. The first storage unit 11 is used to store a software and firmware program or an information F, the first arithmetic unit 12 is used to use, operate or process the software and firmware program or the information F, and the first control unit 13 is used to control operation of the first storage unit 11 and the first arithmetic unit 12. The second module 20 has capability of preventing external intrusion or operating securely, and includes a second storage unit 21, a second decryption unit 22, and a second control unit 23. The second storage unit 21 is used to store an information key, the second decryption unit 22 uses the information key to decrypt the software and firmware program or the information, and the second control unit 23 is used to control operation of the second storage unit 21 and the second decryption unit 22. The first control unit 13 further controls communication between the first module 10 and the second module 20, and the second control unit 23 further controls communication between the second module 20 and the first module 10.

[0009] As shown in FIG. 1, the protection system for software and firmware or information 100 of this embodiment further includes a source end 30, a server 40, an encryptor 50 and a manufacturing end 60. The source end 30 can be a database or a storage device of a software and firmware design company. Software and firmware programs or information designed by the software and firmware company can be sent from the source end 30 to the server 40, transfer of information or data can be performed between the server 40 and the encryptor 50, the server 40 can send the information or data to the manufacturing end 60, and the manufacturing end 60 can be, for example, a burner of a manufacturing plant, capable of burning software and firmware or information into the first module 10.

[0010] The first module 10 can be an integrated circuit chip or other electronic components, the first storage unit 11 of the first module 10 can be a memory in an electronic component, the first arithmetic unit 12 can be an application program or a circuit capable of executing operations, and the first control unit 13 can be a processor for accessing information of the first storage unit 11 or starting the first arithmetic unit 12 to perform operations. The second module 20 can be a security module, and the second storage unit 21 can be a memory. When the first module 10 is started to operate, the first module 10 is connected to the second module 20, and the encrypted software and firmware program or information stored in the first storage unit 11 of the first module 10 can be decrypted by the second module 20 and then sent back to the first module 10, so that the first module 10 can execute or read the decrypted software and firmware program or information to generate a predetermined function.

[0011] Please refer to FIG. 3 to FIG. 6 for one embodiment of a protection method for software and firmware or information of the present invention. As shown in FIGS. 3 and 5, firstly, in step S101, the server 40 obtaining a software and firmware program or an information from the source end 30, for example, the server 40 obtaining the software and firmware program or the information of the source end 30 through a dedicated line or a network; then, in step S102, the server 40 sending the software and firmware program or the information to the encryptor 50;

then, in step S103, the encryptor 50 generating an information key with a random program, and encrypting the software or firmware program or the information with the information key, the random program generating the information key according to a randomly generated random number, the encryptor 50 using the encrypted software or firmware program or information to make a transfer key computation program to generate a transfer key, and then the encryptor 50 encrypting the information key with the transfer key;

then, in step S104, the server 40 obtaining the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program from the encryptor 50;

then, in step S105, the server 40 sending the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program to the manufacturing end 60 (burner);

then, in step S106, the manufacturing end 60 (burner) burning the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program into the first storage unit 11 of the first module 10;

as shown in FIGS. 4 and 6, when the first module 10 is activated, the first module 10 is connected to the second module 20; then, in step S107, the first arithmetic unit 12 using the encrypted software and firmware program or information of the first storage unit 11 to make the transfer key computation program to generate a transfer key, and decrypting the encrypted information key into the information key by using the transfer key; the transfer key computation program can be different corresponding to different types of the first module 10, that is, the transfer key computation program can be different corresponding to different integrated circuit chips;

then, in step S108, the first module 10 sending the information key and the encrypted software and firmware program or information to the second module 20, and storing the information key and the encrypted software and firmware program or information in the second storage unit 21;

then, in step S109, the second decryption unit 22 decrypting the encrypted software and firmware program or information by using the information key to obtain the decrypted software and firmware program or information;

then, in step S110, sending the decrypted software and firmware program or information from the second module 20 to the first module 10 and storing the decrypted software and firmware program or information in the first storage unit 11; and

then, in step Sill, the first module 10 deleting the information key and the transfer key computation program from the first storage unit 11.

[0012] Since the second module 20 corresponding to the first module 10 does not have operation function, in addition to the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program being burned into the first module 10 together, when the encrypted information key needs to be decrypted, the first arithmetic unit 12 of the first module 10 can execute the transfer key computation program to decrypt the encrypted information key.

[0013] Please refer to FIGS. 7 and 8 for another embodiment of the protection system for software and firmware or information of the present invention. A protection system for software and firmware or information 200 of this embodiment includes a third module 70 and a fourth module 80. The third module 70 includes a third storage unit 71, a third arithmetic unit 72, and a third control unit 73. The third storage unit 71 is used to store a software and firmware program or an information, the third arithmetic unit 72 is used to use, operate or process the software and firmware program or the information, and the third control unit 73 is used to control the third storage unit 71 and the third arithmetic unit 72. The fourth module 80 has capability of preventing external intrusion or operating securely, and includes a fourth storage unit 81, a fourth decryption unit 82, a fifth storage unit 83, a fourth arithmetic unit 84, and a fourth control unit 85. The fourth storage unit 81 is used to store an information key, and the fourth decryption unit 82 uses the information key to decrypt the software and firmware program or the information. The fifth storage unit 83 is used to store a software and firmware program or an information. The fourth arithmetic unit 84 is used to use, operate or process the software and firmware program or the information. The fourth control unit 85 is used to control operation of the fourth storage unit 81, the fourth decryption unit 82, the fifth storage unit 83, and the fourth arithmetic unit 84. The third control unit 73 further controls communication between the third module 70 and the fourth module 80, and the fourth control unit 85 further controls communication between the fourth module 80 and the third module 70.

[0014] In this embodiment, the source end 30, the server 40, the encryptor 50, and the manufacturing end 60 are the same as those of the embodiment shown in FIG. 1, and thus will not be repeated here. The difference between this embodiment and the embodiment of FIGS. 1 to 6 is that the fourth module 80 of this embodiment has arithmetic capability, so operation of decryption is performed in the fourth module 80.

[0015] Please refer to FIG. 9 to FIG. 14 for another embodiment of the protection method for software and firmware or information of the present invention. As shown in FIG. 9, firstly, in step S201, the server 40 obtaining a software and firmware program or an information from the source end 30, for example, the server 40 obtaining the software and firmware program or the information of the source end 30 through a dedicated line or a network;

then, in step S202, the server 40 sending the software and firmware program or the information to the encryptor 50;

then, in step S203, the encryptor 50 generating an information key with a random program, and encrypting the software or firmware program or the information with the generated information key, the random program generating the information key according to a randomly generated random number, the encryptor 50 using the encrypted software or firmware program or information to make a transfer key computation program to generate a transfer key, and then the encryptor 50 encrypting the information key with the transfer key;

then, in step S204, the server 40 obtaining the encrypted software and firmware program or information, and the

encrypted information key from the encryptor 50;
then, in step S205, the server 40 sending the encrypted software and firmware program or information, and the encrypted information key to the manufacturing end 60 (burner);
then, in step S206, the manufacturing end 60 (burner) burning the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program into the third storage unit 71 of the third module 70;
as shown in FIGS. 10 and 13, then in step S207, the server 40 obtaining the transfer key computation program from the encryptor 50;
then, in step S208, the server 40 sending the transfer key computation program to the manufacturing end 60 (burner);
then, in step S209, the manufacturing end 60 (burner) burning the transfer key computation program into the fifth storage unit 83 of the fourth module 80;
as shown in FIGS. 11 and 14, then in step S210, the third module 70 sending the encrypted software and firmware program or information to the fourth module 80;
then, in step S211, the fourth arithmetic unit 84 generating a transfer key with the encrypted software and firmware program or information and by using the transfer key computation program;
then, in step S212, the third module 70 sending the encrypted information key to the fourth module 80;
then, in step S213, the fourth decryption unit 82 using the transfer key to decrypt the encrypted information key into an information key, and storing the information key in the fourth storage unit 81;
then, in step S214, the fourth decryption unit 82 decrypting the encrypted software and firmware program or information with the decrypted information key; and
then, in step S215, sending the decrypted software and firmware program or information from the fourth module 80 to the third module 70 and storing the decrypted software and firmware program or information in the third storage unit 71.

[0016] The protection system and the protection method for software and firmware or information of the present invention are capable of encrypting and adding software and firmware or information to an electronic component, so that the software and firmware or the information is protected during the process of burning into the electronic component at the manufacturing end. Even if the encrypted software and firmware or information is obtained, the original content thereof cannot be acquired. When the electronic component is activated and used, the software and firmware or the information stored therein is then decrypted. In this way, the software and firmware or the information in the electronic component can be protected from being stolen, and the cost of the electronic component can be reduced and is easy to promote.

[0017] It is to be understood that the above description is only preferred embodiments of the present invention and is not used to limit the present invention, and changes in accordance with the concepts of the present invention may be made without departing from the spirit of the present invention, for example, the equivalent effects produced by various transformations, variations, modifications and applications made to the configurations or arrangements shall still fall within the scope covered by the appended claims of the present invention.

Claims

1. A protection system for software and firmware or information including:

a first module including:

a first storage unit for storing a software and firmware program or an information;
a first arithmetic unit for using, operating or processing the software and firmware program or the information; and
a first control unit for controlling operation of the first storage unit and the first arithmetic unit; and

a second module with capability of preventing external intrusion or operating securely, including:

a second storage unit for storing an information key;
a second decryption unit using the information key to decrypt the software and firmware program or the information; and
a second control unit for controlling operation of the second storage unit and the second decryption unit;

wherein the first control unit further controls communication between the first module and the second module, and the second control unit further controls communication between the second module and the first module.

2. The protection system for software and firmware or information as claimed in claim 1, wherein the second decryption unit decrypts the software and firmware program or the information with the information key in the second module.

3. The protection system for software and firmware or information as claimed in claim 2, wherein the software and firmware program or the information decrypted with the information key is operated by the first arithmetic unit.

4. A protection method for software and firmware or information including:

a server obtaining a software and firmware program or an information from a source end;
the server sending the software and firmware program or the information to an encryptor;
the encryptor generating an information key;
the encryptor using the information key to encrypt the software and firmware program or the information into an encrypted software and firmware program or information;
the encryptor using the encrypted software or firmware program or information to make a transfer key computation program to generate a transfer key;
the encryptor using the transfer key to encrypt the information key into an encrypted information key;
the server obtaining the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program from the encryptor;
the server sending the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program to a burner;
the burner burning the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program into the first storage unit of the first module as claimed in claim 1;
the first arithmetic unit as claimed in claim 1 using the encrypted software and firmware program or information of the first storage unit to make the transfer key computation program to generate the transfer key, and decrypting the encrypted information key into the information key by using the transfer key;
the first module as claimed in claim 1 sending the information key to the second module, and storing the information key in the second storage unit; and
the first control unit as claimed in claim 1 deleting the transfer key computation program and the information key of the first storage unit.

5. The protection method for software and firmware or information as claimed in claim 4, wherein after the information key is sent to the second module, the first control unit deletes the encrypted information key of the first storage unit.

6. A protection system for software and firmware or information including:

a third module including:

a third storage unit for storing a software and firmware program or an information;
a third arithmetic unit for using, operating or processing the software and firmware program or the information; and
a third control unit for controlling the third storage unit and the third arithmetic unit; and

a fourth module with capability of preventing external intrusion or operating securely, including:

a fourth storage unit for storing an information key;
a fourth decryption unit using the information key to decrypt the software and firmware program or the information;
a fifth storage unit for storing a software and firmware program;
a fourth arithmetic unit for using, operating or processing the software and firmware program; and
a fourth control unit for controlling operation of the fourth storage unit, the fourth decryption unit, the fifth storage unit and the fourth arithmetic unit;

wherein the third control unit further controls communication between the third module and the fourth module, and the fourth control unit further controls communication between the fourth module and the third module.

7. The protection system for software and firmware or information as claimed in claim 6, wherein the fourth decryption unit decrypts the software and firmware program or the information with the information key in the fourth module.

8. The protection system for software and firmware or information as claimed in claim 7, wherein the software and firmware program or the information decrypted with the information key is operated by the fourth arithmetic unit.

9. A protection method for software and firmware or information including:

a server obtaining a software and firmware program or an information from a source end;
the server sending the software and firmware program or the information to an encryptor;
the encryptor generating an information key;
the encryptor using the information key to encrypt the software and firmware program or the information into an encrypted software and firmware program or information;
the encryptor using the encrypted software or firmware program or information to make a transfer key computation program to generate a transfer key;

using the transfer key to encrypt the information key into an encrypted information key;
the server obtaining the encrypted software and firmware program or information, and the encrypted information key from the encryptor;
the server sending the encrypted software and firmware program or information, and the encrypted information key to a burner;
the burner burning the encrypted software and firmware program or information, and the encrypted information key into the third storage unit of the third module as claimed in claim 6;
the server obtaining the transfer key computation program from the encryptor;
the server sending the transfer key computation program to a burner;
the burner burning the transfer key computation program into the fifth storage unit of the fourth module as claimed in claim 6;
the third module as claimed in claim 6 sending the encrypted software and firmware program or information to the fourth module;
the fourth arithmetic unit as claimed in claim 6 using the encrypted software and firmware program or information to make the transfer key computation program to generate the transfer key;
the third module as claimed in claim 6 sending the encrypted information key to the fourth module; and
the fourth decryption unit as claimed in claim 6 using the transfer key to decrypt the encrypted information key into an information key, and storing the information key in the fourth storage unit.

10. The protection method for software and firmware or information as claimed in claim 9, wherein the third control unit deletes the encrypted information key of the third storage unit.

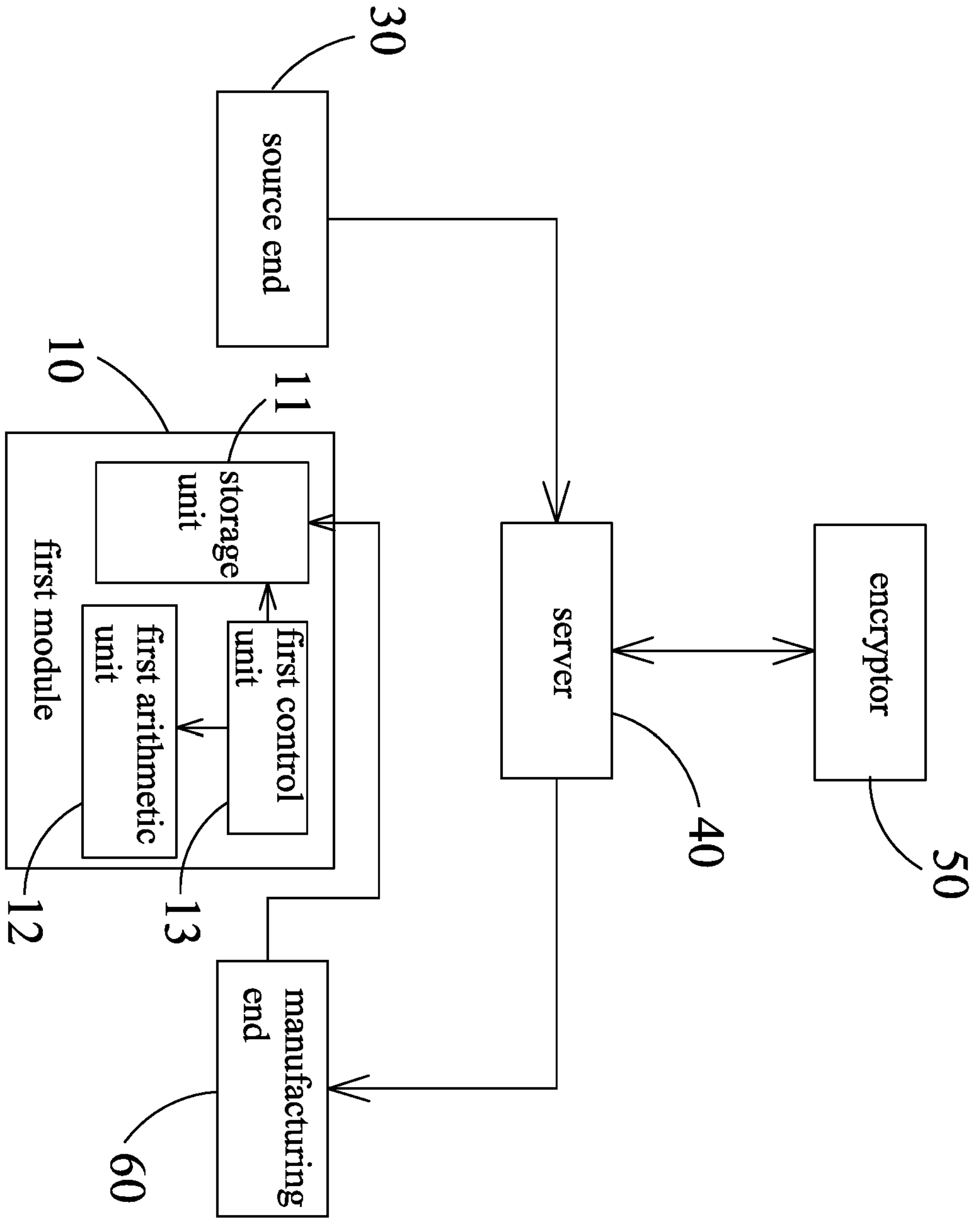
source end
30
first module
10
storage unit
11
first control unit
13
first arithmetic unit
12
server
40
encryptor
50
manufacturing end
60

FIG. 1

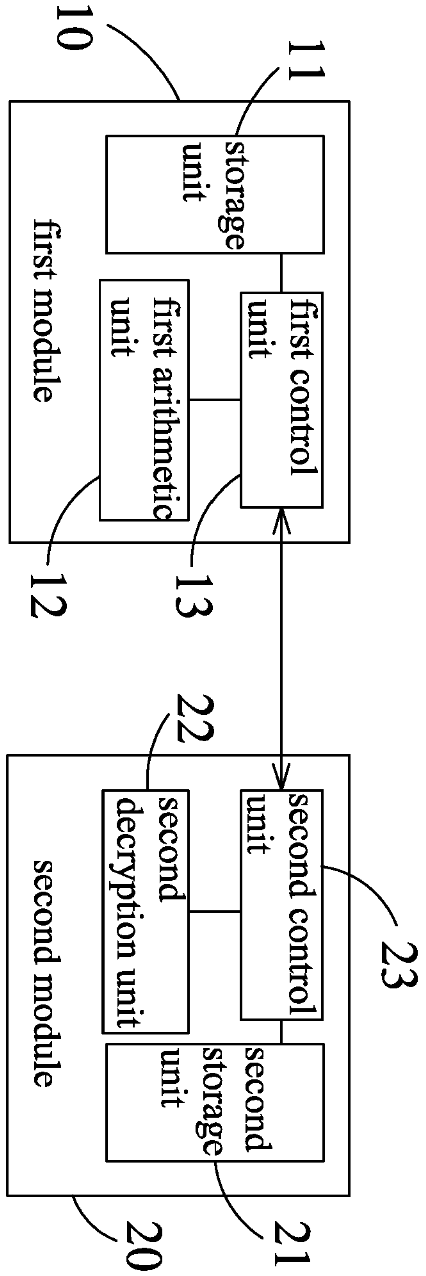
10
11
storage unit
first module
first control unit
first arithmetic unit
12
13
22
second control unit
second decryption unit
second module
second storage unit
23
20
21

FIG. 2

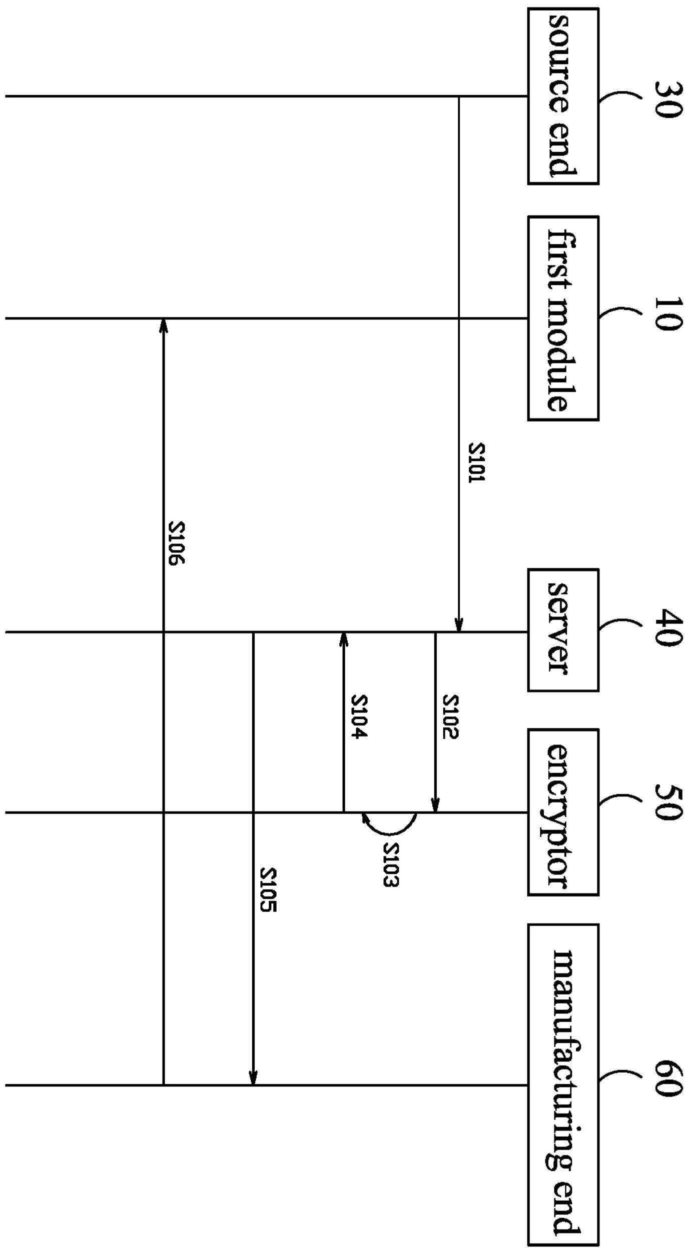
30
source end
10
first module
40
server
50
encryptor
60
manufacturing end
S101
S102
S103
S104
S105
S106

FIG. 3

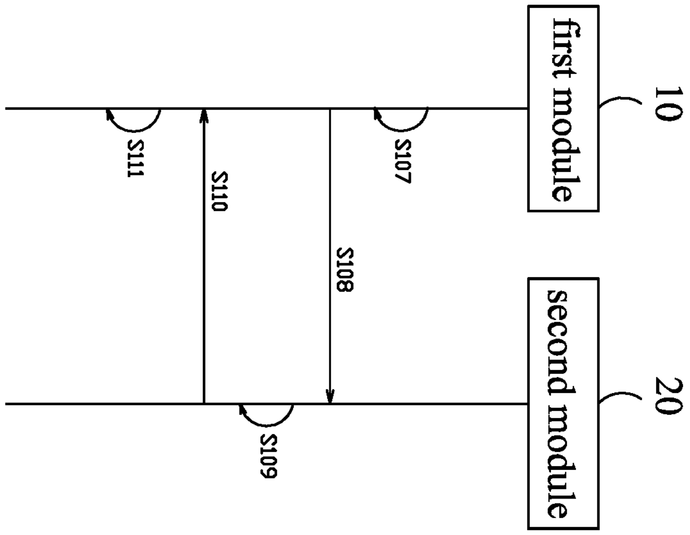

FIG. 4

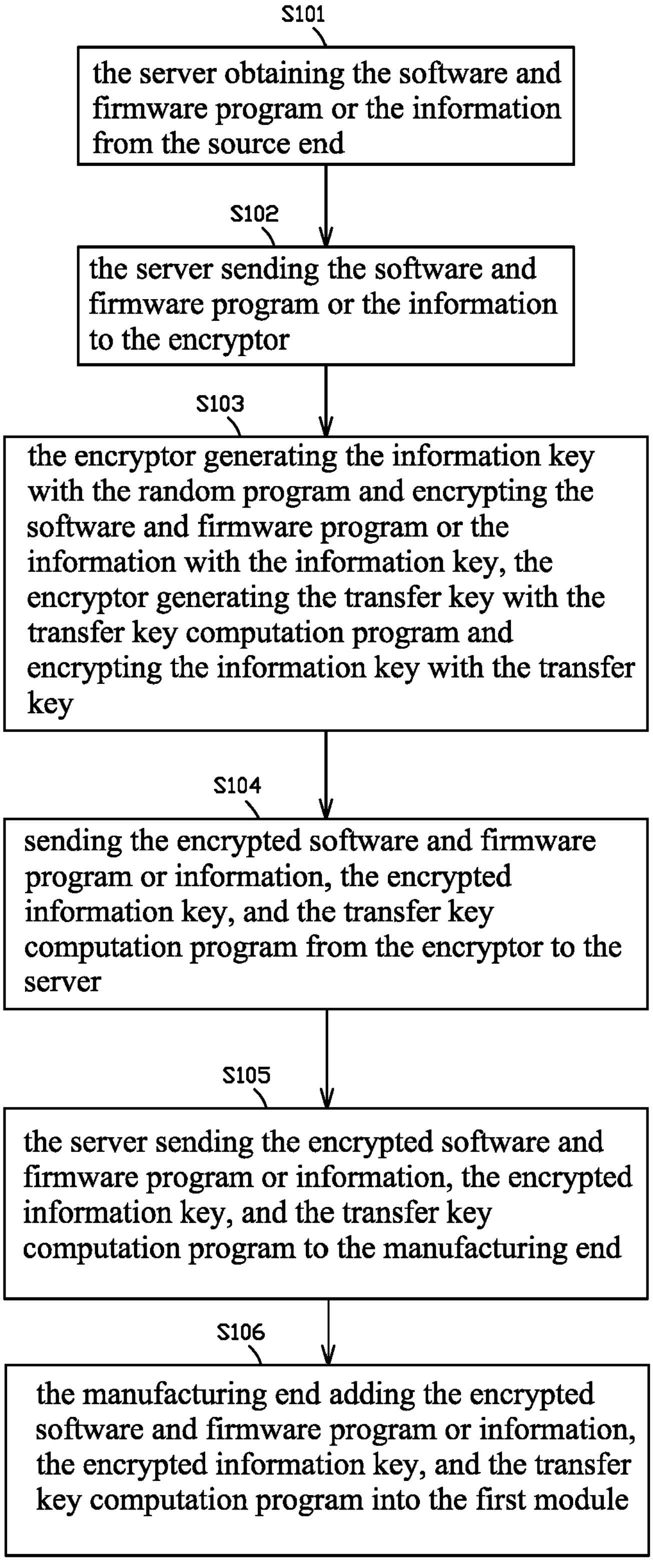
S101
the server obtaining the software and firmware program or the information from the source end
S102
the server sending the software and firmware program or the information to the encryptor
S103
the encryptor generating the information key with the random program and encrypting the software and firmware program or the information with the information key, the encryptor generating the transfer key with the transfer key computation program and encrypting the information key with the transfer key
S104
sending the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program from the encryptor to the server
S105
the server sending the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program to the manufacturing end
S106
the manufacturing end adding the encrypted software and firmware program or information, the encrypted information key, and the transfer key computation program into the first module

FIG. 5

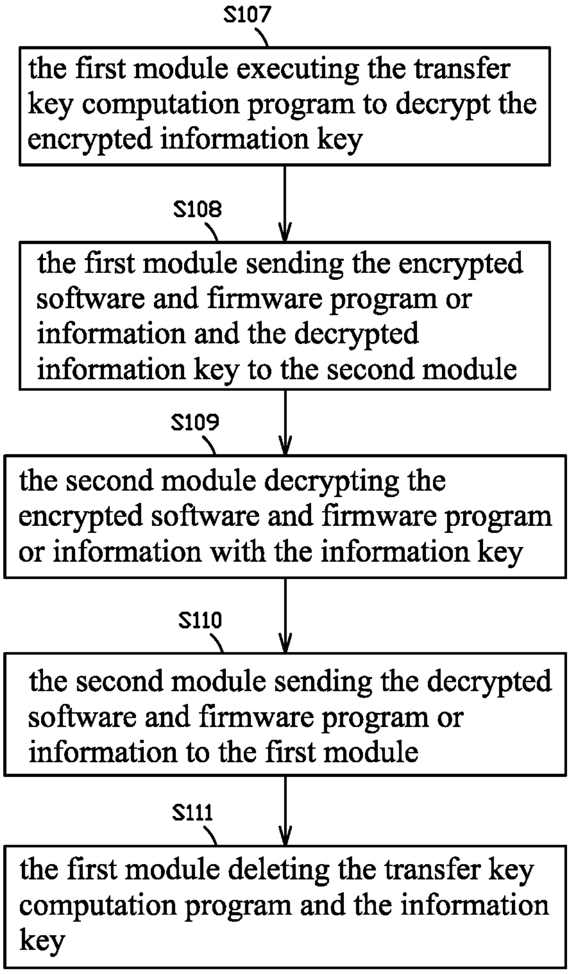
S107
the first module executing the transfer key computation program to decrypt the encrypted information key
S108
the first module sending the encrypted software and firmware program or information and the decrypted information key to the second module
S109
the second module decrypting the encrypted software and firmware program or information with the information key
S110
the second module sending the decrypted software and firmware program or information to the first module
S111
the first module deleting the transfer key computation program and the information key

FIG. 6

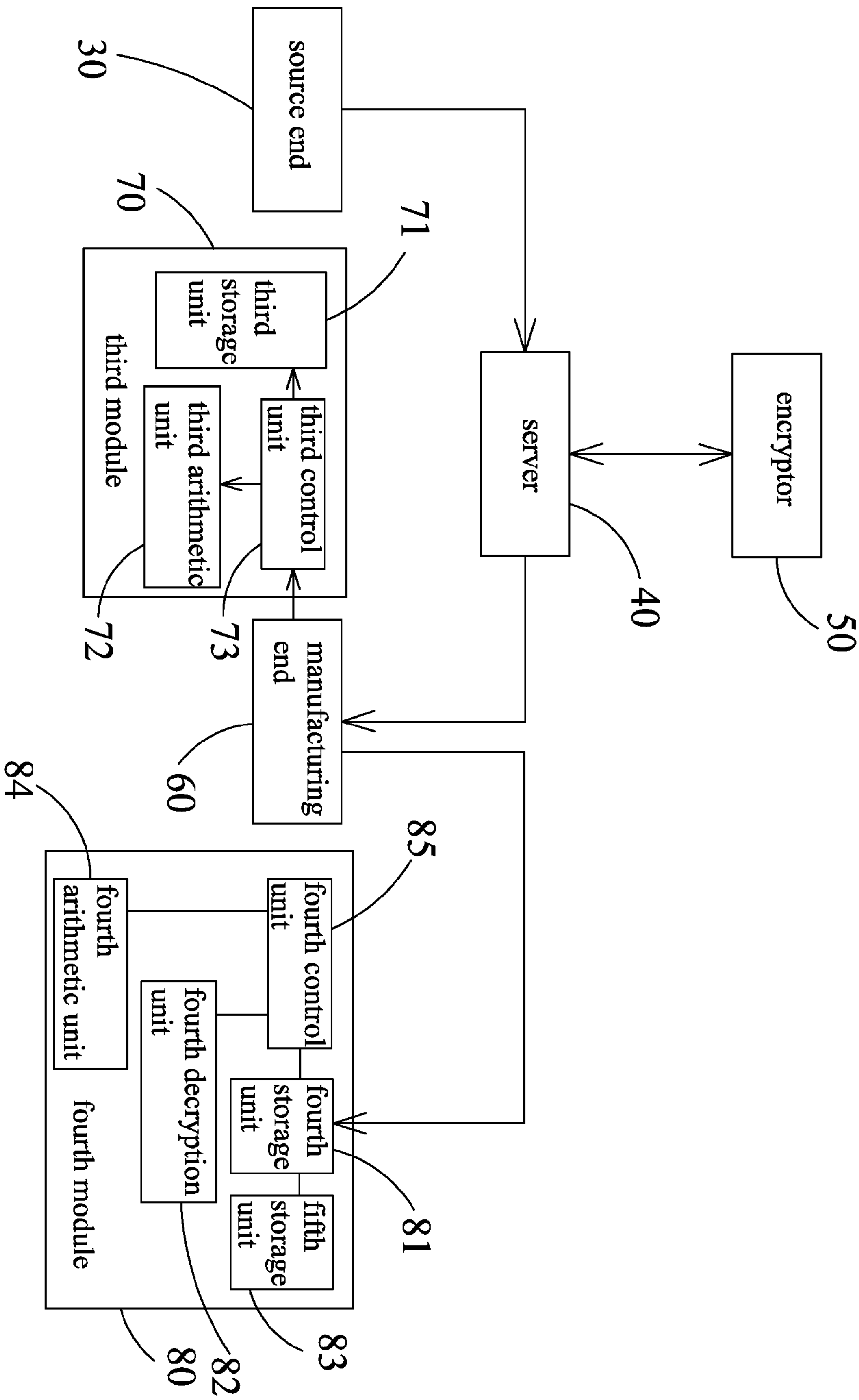
source end
30
server
40
encryptor
50
70
third module
third storage unit
71
third control unit
73
third arithmetic unit
72
manufacturing end
60
84
fourth arithmetic unit
85
fourth control unit
fourth decryption unit
82
fourth storage unit
81
fifth storage unit
83
fourth module
80

FIG. 7

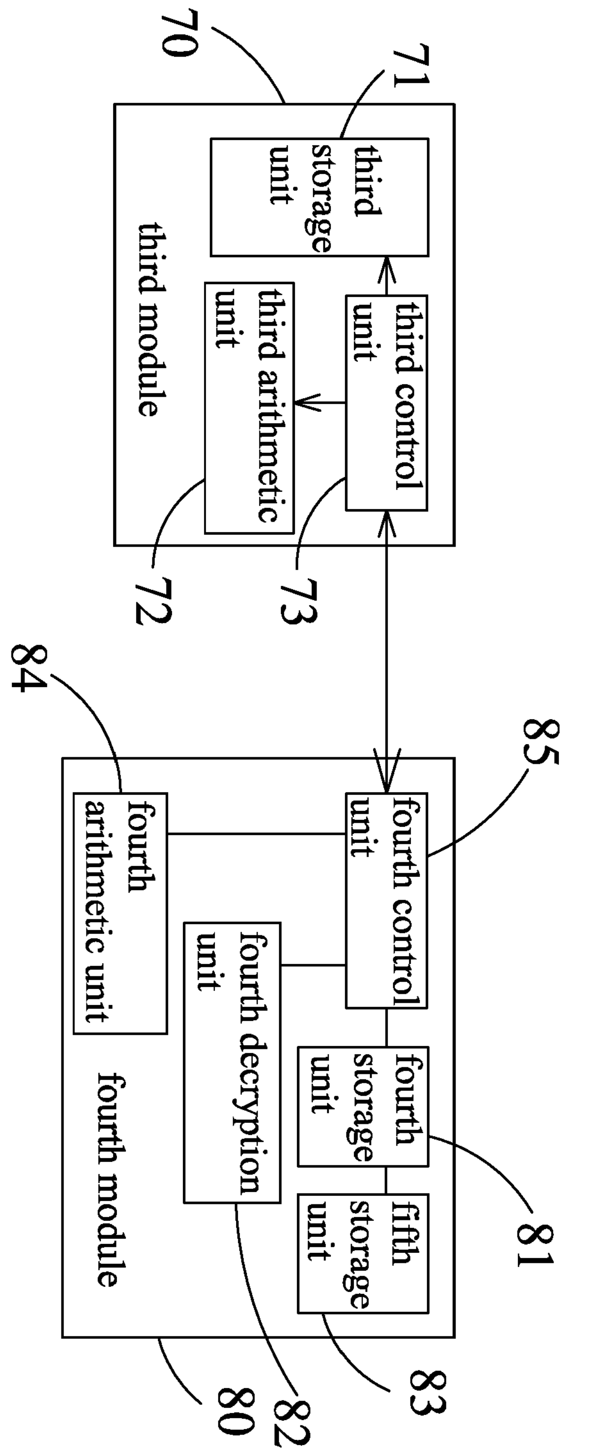
70
71
third storage unit
third module
third control unit
third arithmetic unit
72
73
84
85
fourth control unit
fourth arithmetic unit
fourth decryption unit
fourth storage unit
fifth storage unit
fourth module
81
83
82
80

FIG. 8

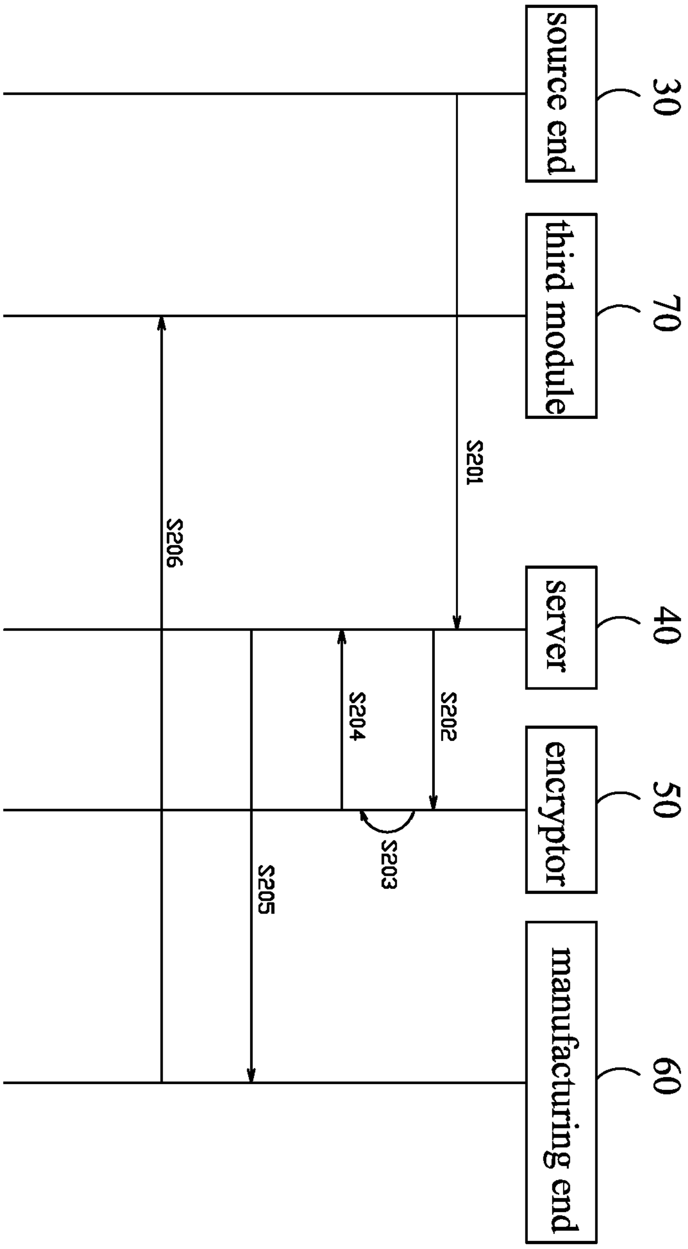
30
source end
70
third module
40
server
50
encryptor
60
manufacturing end
S201
S202
S203
S204
S205
S206

FIG. 9

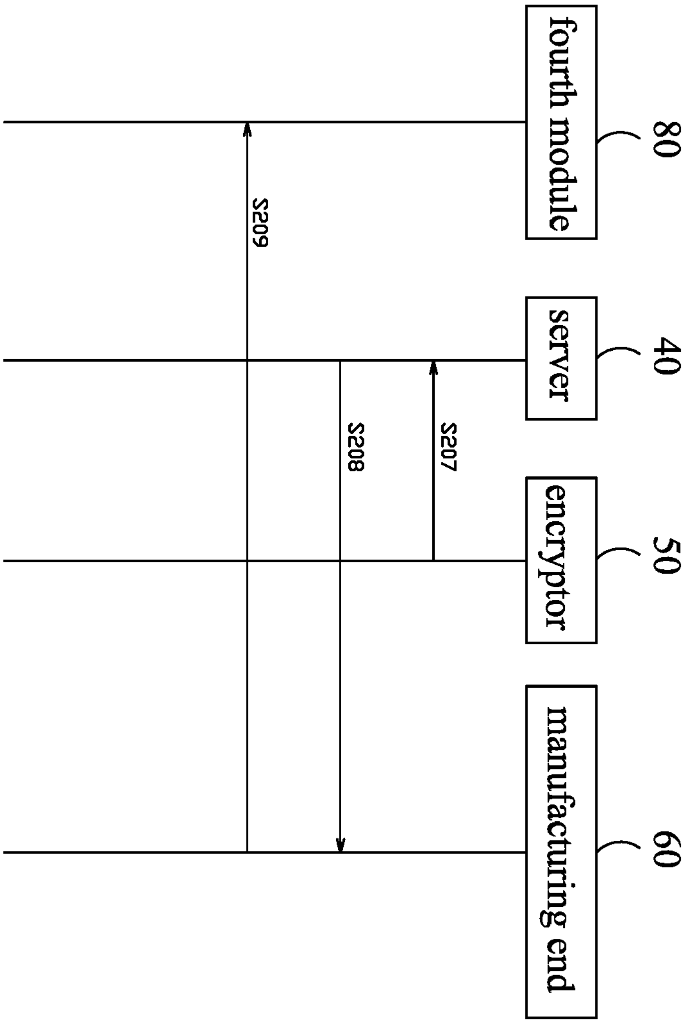
80
fourth module
40
server
50
encryptor
60
manufacturing end
S207
S208
S209

FIG. 10

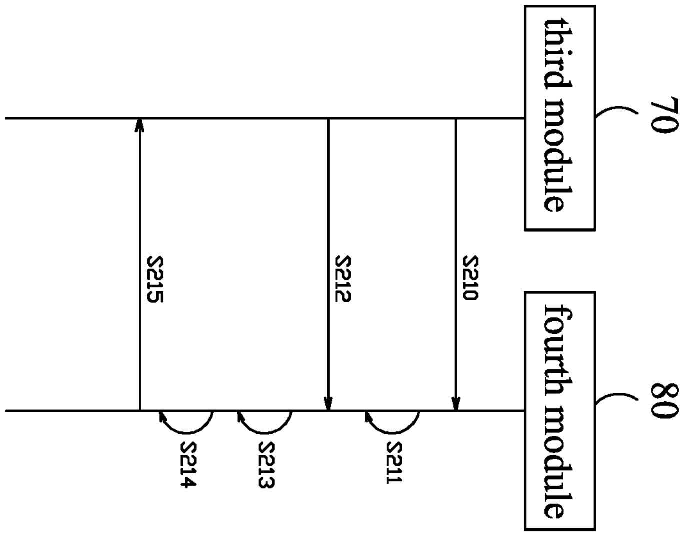
70
third module
80
fourth module
S210
S211
S212
S213
S214
S215

FIG. 11

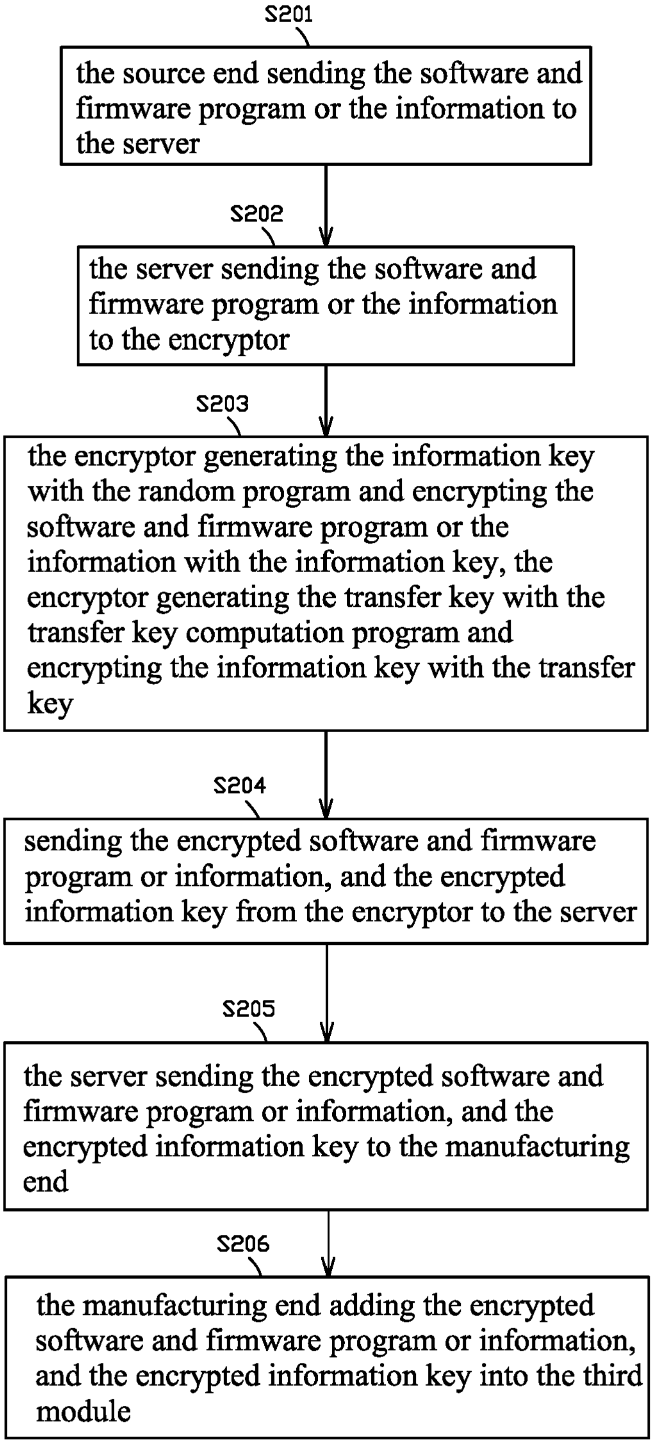
S201
the source end sending the software and firmware program or the information to the server
S202
the server sending the software and firmware program or the information to the encryptor
S203
the encryptor generating the information key with the random program and encrypting the software and firmware program or the information with the information key, the encryptor generating the transfer key with the transfer key computation program and encrypting the information key with the transfer key
S204
sending the encrypted software and firmware program or information, and the encrypted information key from the encryptor to the server
S205
the server sending the encrypted software and firmware program or information, and the encrypted information key to the manufacturing end
S206
the manufacturing end adding the encrypted software and firmware program or information, and the encrypted information key into the third module

FIG. 12

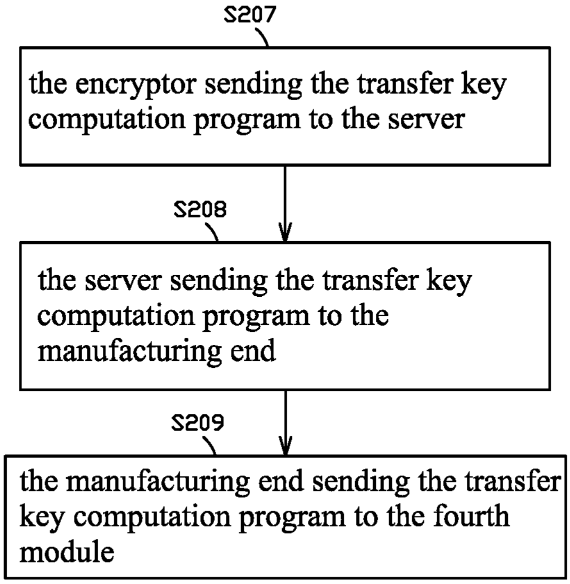
S207
the encryptor sending the transfer key computation program to the server
S208
the server sending the transfer key computation program to the manufacturing end
S209
the manufacturing end sending the transfer key computation program to the fourth module

FIG. 13

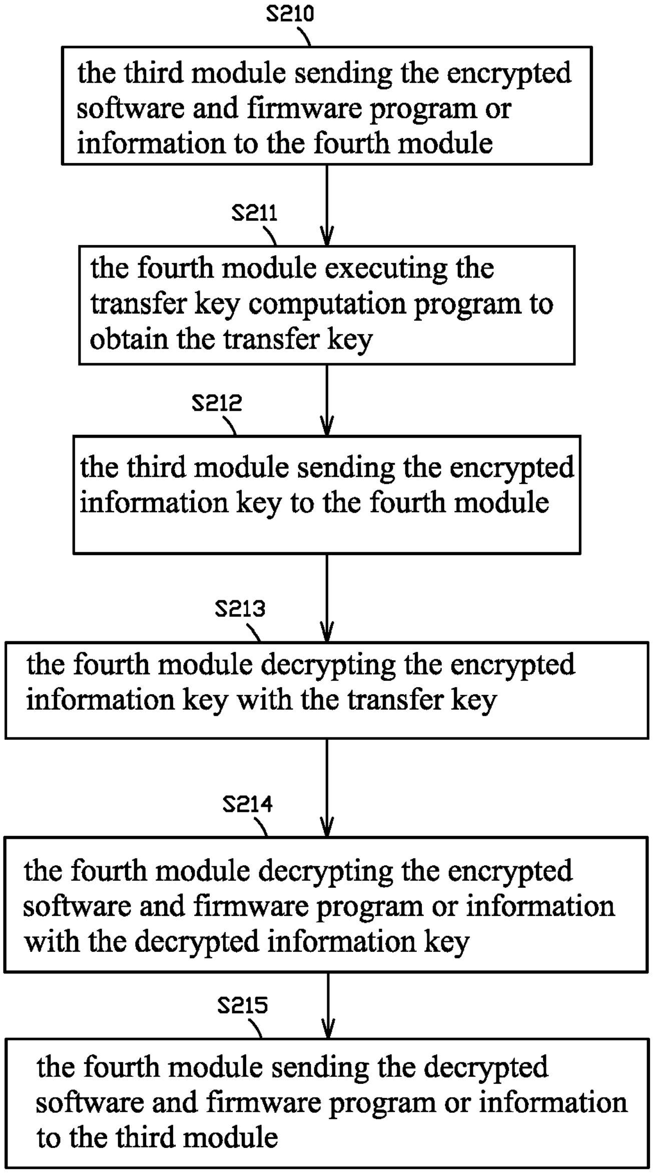
S210
the third module sending the encrypted software and firmware program or information to the fourth module
S211
the fourth module executing the transfer key computation program to obtain the transfer key
S212
the third module sending the encrypted information key to the fourth module
S213
the fourth module decrypting the encrypted information key with the transfer key
S214
the fourth module decrypting the encrypted software and firmware program or information with the decrypted information key
S215
the fourth module sending the decrypted software and firmware program or information to the third module

FIG. 14

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 20 21 7643

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X A	US 2014/082373 A1 (COLNOT VINCENT CEDRIC [BE]) 20 March 2014 (2014-03-20) * paragraph [0030] - paragraph [0048]; figures 2a,2b,4a,4b,5 * -----	1-3,6-10 4,5	INV. G06F21/57 G06F8/61 H04L9/08
A	US 2018/069852 A1 (BUENDGEN REINHARD T [DE] ET AL) 8 March 2018 (2018-03-08) * paragraph [0001] - paragraph [0019]; figures 1-3 * -----	1-10	
A	US 2011/035587 A1 (DEVORE SCOTT [US] ET AL) 10 February 2011 (2011-02-10) * paragraph [0028] - paragraph [0078]; figures 1-5 * -----	1-10	

TECHNICAL FIELDS SEARCHED (IPC)
G06F
H04L

The present search report has been drawn up for all claims

1

Place of search	Date of completion of the search	Examiner
Munich	9 June 2021	Mäenpää, Jari

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 20 21 7643

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-06-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014082373 A1	20-03-2014	CN 103679004 A	26-03-2014
		EP 2711858 A1	26-03-2014
		US 2014082373 A1	20-03-2014
US 2018069852 A1	08-03-2018	US 9454662 B1	27-09-2016
		US 9471786 B1	18-10-2016
		US 9536095 B1	03-01-2017
		US 9563753 B1	07-02-2017
		US 2017111354 A1	20-04-2017
		US 2018069852 A1	08-03-2018
US 2011035587 A1	10-02-2011	US 2011035587 A1	10-02-2011
		WO 2011017624 A2	10-02-2011

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82