

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 December 2006 (28.12.2006)

PCT

(10) International Publication Number
WO 2006/136881 A1

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/IB2005/052051

(22) International Filing Date: 22 June 2005 (22.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):
FREESCALE SEMICONDUCTOR, INC. [US/US];
7700 West Parmer Lane, Austin, TX 78729 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **DAHAN, Odi** [IL/IL]; Hatabak 7, 44813 Oranit (IL). **GOREN, Ori** [IL/IL]; Kibutz Ruchama, 79180 Kibutz Ruchama (IL). **SHVAGER, Yehuda** [IL/IL]; Hagefen 13 PO BOX 1728, 73127 Chashmona'im (IL).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

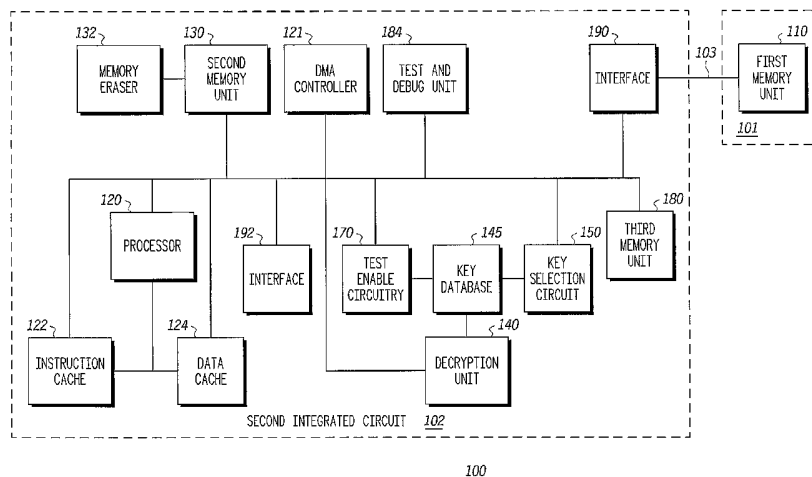
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DEVICE AND METHOD FOR SECURING SOFTWARE



(57) Abstract: A device (100) that includes a first memory unit (110) adapted to store encrypted instructions, a processor (120) adapted to execute decrypted instructions, a second memory unit (130) accessible by the processor (120), and a decryption unit (140). The device (100) is characterized by including a key database (145) and a key selection circuit (150), wherein the key selection circuit (150) is adapted to select a selected decryption key from the key database (145) for decrypting encrypted instructions. The selection is responsive to a fixed selection information stored within the integrated circuit and to received key selection information. A method (200) that includes a stage of receiving (230) encrypted instructions; and executing (290) decrypted instructions by a processor. The method is characterized by receiving (240) key selection information, selecting (260) a selected decryption key out of a key database in response to fixed selection information and to the received key selection information, and decrypting (270) encrypted instructions using the selected decryption key.



WO 2006/136881 A1

DEVICE AND METHOD FOR SECURING SOFTWARE

FIELD OF THE INVENTION

The present invention relates to devices and methods
5 for securing software.

BACKGROUND OF THE INVENTION

Modern electrical circuits include software and
hardware components. In many cases the software is copied
10 in order to save development cost. The cloned software
can be used by third parties on the same hardware
platform that did not invest in developing the software
and can provide cheaper products than the original
developer of the software.

15 The hackers can download the software in various
manners, and can even use devices testing and debugging
capabilities to learn about the software. .

Various attempts were made to prevent software
cloning and/or to secure integrated circuits. U.S. patent
20 application number 2003/0177373 of Moyer et al., titled
"Integrated circuit security and method therefore", which
is incorporated herein by reference, describes an
integrated circuit that provides a security key base
integrated circuit protection scheme.

25 U.S. patent 5898776 of Apland et al. titled
"security antifuse that prevents readout of some but not
other information from a programmed field programmable
gate array", which is incorporated herein by reference,
describes an antifuse that can be programmed to disable
30 access to a JTAG boundary scan register, while allowing
access to a JTAG bypass register.

U.S. patent 5091942 of Dent, titled "Authentication
system for digital cellular communication", which is

incorporated herein by reference, describes a system and method that is used for authenticating mobile stations and base stations in a cellular communication network that uses a rolling key that includes historical
5 information.

U.S. patent 6158005 of Bharathan et al., titled "Cloning protection scheme for a digital information playback device", which is incorporated herein by reference, describes a method and apparatus for cloning
10 protection of a player. A unique identifier is required in order to enable the playback. The unique identifier is communicated to a server.

U.S. patent application publication serial number 2003/0061488 of Huebler et al., titled "Cloning
15 protection for electronic equipment" which is incorporated herein by reference, describes a method and apparatus for protecting electronic devices from cloning that employ and electronic signature generated from an identification code for the electronic device, an
20 international mobile equipment identifier, and a unique unchangeable identification for a hardware component of the electronic device code.

There is a need to provide efficient method and device for cloning protection and reverse engineering
25 prevention.

SUMMARY OF THE PRESENT INVENTION

A device and a method for securing software, as described in the accompanying claims.

30

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed

description taken in conjunction with the drawings in which:

FIG. 1 illustrates a device according to an embodiment of the invention;

5 FIG. 2 illustrates a test enable circuit, a decryption unit, a key database and a key selection circuit, according to an embodiment of the invention;

10 FIG. 3-7, and FIG. 9 illustrate a device booting sequence, according to an embodiment of the invention; and

FIG. 8 illustrates a method, according to an embodiment of the invention.

15 DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Various figures illustrate non-limiting exemplary configurations of a device for securing software. It is noted that other configurations can be used without departing from the scope of the invention. For example, 20 the amount of memory units that store the encrypted information may exceed one, the amount of integrated circuits within a device may differ than two, the amount of processors within a second integrated circuit may exceed one, and the like.

25 According to an embodiment of the invention a unique encryption key is used to encrypt instructions. The integrated circuit manufacturer can allow a first customer to access one set of keys and allow another customer to access a different set of keys, and thus 30 prevent one customer from cloning the decrypted software of the other customer.

FIG. 1 illustrates a device 100, according to an embodiment of the invention.

Device 100 includes a first integrated circuit 101 and a second integrated circuit 102. The first integrated circuit 101 is connected to the second integrated circuit 102 by a bus 103.

5 Conveniently, the first integrated circuit 101 includes a first memory unit 110 that stores encrypted instructions.

 The second integrated circuit 102 includes processor 120, second memory unit 130, memory eraser 132, a
10 decryption unit 140, key database 145, key selection circuit 150, instruction cache 122, data cache 124, a third memory unit 180, a test and debug unit 184, and I/O interfaces 190 and 192.

 According to an embodiment of the invention the key
15 database is spread in a large area of the integrated circuit, and combined with various logic circuits, such as avoid microscopic detection of the keys.

 The memory eraser 132 can be a part of the second memory unit 130. Conveniently it is a part of a built in
20 self test (BIST) unit. It is capable of erasing one or more entries of the second memory unit 130. The erasure conveniently occurs in response to commands or control signals provided by the processor 120. The erasure of memory entries can be included in a booting sequence of
25 the device 100.

 It is further noted that processor 120 can erase the second memory unit 130 but it is usually more efficient to use a memory eraser 132 while allowing the processor 120 to handle other tasks. It is further noted that other
30 components, such as a DMA controller 121, can also erase the entries of the second memory unit 130.

 The second memory unit 130 stores decrypted instructions and can also store these instructions in an

encrypted format, before they are decrypted by decryption unit 140. It is noted that the second integrated circuit 102 can include multiple memory units for storing encrypted an/or decrypted instructions.

5 The processor 120, second memory unit 120, test and debug unit 184, interface 190, third memory unit 180, key selection circuit 150, test enable circuit 170, decryption unit 140, and interface 192 are connected to each other by a bus or a interconnecting mesh. It is
10 noted that these components can be connected in various manners and that a DMA or other type of memory transfer controller or media access controller can manage the traffic over the bus or mesh.

15 It is further noted that the test and debug unit 184 can be split to a test unit and to a debug unit and that only one of said units can be included within the second integrated circuit 102 via interface 92. Interface 192 expects to read only the key. If the key does not match then the device will reset to avoid brute force attack.
20 Conveniently, a test session or a debug session can initiate only if a user provides a selected decryption key to the second integrated circuit 102 .

25 Conveniently, the key database 140, the key selection circuit 150 can not be accessed from outside the second integrated circuit 102, either by direct access, by testing or by debugging.

30 Conveniently, the access to the second memory unit 130 is limited such as to allow a test unit to read a certain entry of the second memory unit 130 only if that test unit has already written to this entry.

 Conveniently, the instruction cache 122 and/or the data cache 124 are invalidated during a booting session or otherwise are configured not to provide content that

was written to them before certain events (such as a reset) occurred.

Device 100 can include many interfaces.

Conveniently, these interfaces are not direct access
5 interfaces but rather controlled by processor 120. The control can be implemented by buffer descriptors or by single instructions. If device 100 includes some or more direct access interface than they are limited to certain memory spaces that do not include, for example, the
10 second memory unit 130 or other entries that include decrypted instructions, or device 102 internal registers.

Conveniently, one interface, such as interface 190 is relatively slow, while the other interface 192 is relatively fast. The inventors used a slow I²C interface
15 and a fast Ethernet interface, although other interface adapted to other communication protocols can be utilized. Encrypted data or instructions can be retrieved via one or more of these interfaces.

The key selection circuit 150 is adapted to select a
20 selected decryption key from the key database 145 for decrypting encrypted instructions. The selection is responsive to a fixed selection information stored within the integrated circuit and to received key selection information.

25 The fixed selection information can be set by the manufacturer of the second integrated circuit 102. Each client can receive a different fixed selection information, without knowing this fixed selection information and without knowing the fixed selection
30 information of other clients.

Conveniently, the fixed selection information can be implemented by fuses and the like. It is should not be a

part of any scan chain and can not be either tested or debugged.

Conveniently, each fixed selection information can select a certain group of keys within the key database
5 145. Different fixed selection information conveniently do not enable a user to select the same encryption key.

The fixed selection information can be implemented by fuses, pull down circuits and/or pull up circuits and the like. It is conveniently hidden from a user. For
10 example, it is not a part of any scan chain and can not be either tested or debugged.

Even if a user knows the received key selection information, he will not be able to decrypt the software because he can not access that key, regardless of the key
15 information he feeds to the key selection circuit 145.

According an embodiment of the invention the encrypted instructions are also hashed before being stored in the first memory unit 110. Conveniently the encrypted instructions are hashed such as to allow the
20 second integrated circuit 102 to check that the encrypted instructions were not tampered or altered by a third party.

Conveniently, the hashing utilizes the selected decryption key.

25 Conveniently, the encryption unit 140 does not fetch the whole bulk of encrypted instructions at once, but it rather fetches instruction groups. Conveniently, the hashing is applied on groups of instructions. This allows the encryption unit 140 to perform de-hashing operations
30 on a group of instructions before encrypting these instructions.

Those of skill in the art will appreciate that the hashing can be applied on multiple instruction that

differ by size from the size of the instruction groups
fetches by the decryption unit 140.

According to another embodiment of the invention the
de-hashing is executed by a component that differs from
5 the decryption unit 140. If one unit performs decryption
and another performs de-hashing than these units can
operate in a pipelined manner. According to a further
embodiment of the invention other integrity checking
schemes are applied.

10 According to an embodiment of the invention the
encrypted instructions (or at least some of these
instructions) are decrypted during a booting session of
the second integrated circuit 102. The booting session
can start by retrieving an initial booting code from the
15 third memory unit 180 (that can be a ROM type memory
unit). The execution of the initial booting code
initiates the decryption session.

According to yet another embodiment of the invention
the processor 120 does not execute code unless it is
20 provided from certain locations, such as from the first
memory unit 110. Conveniently, even if the instruction
was retrieved from a predefined location it is de-hashed
and only if the de-hashing stage was successful it is
decrypted and only then executed.

25 FIG. 2 illustrates a test enable circuit 170, a
decryption unit 140, a key database 145 and a key
selection circuit 150, according to an embodiment of the
invention.

The key selection circuit 150 includes a register
30 151 that has a fixed portion 152 and multiple cells 153.
The cells 153 are connected to logic 154 that is adapted
to provide a default value until key selection
information is received by the second integrated circuit

102. Logic 154 is also adapted to limit the amount of writing attempts to register 151, and conveniently limits this amount to a single writing attempt after reset. Various logical circuits can be utilized in order to provide this functionality.

The default value can be written to the register during a booting sequence, but can also be set by dedicated hardware. The default value points to a default key that differs from the encryption key.

It is noted that additional attempts to write to the register 151 can cause the system 100 to halt, to generate an intrusion attempt alert, to disregard the attempt, to provide the default key, and the like.

The register 151 points to one entry of the key database 145 and selects one encryption key out of the multiple keys of that database. Each key differs from the other. The selected encryption key can be sent to a selected key register 158.

The inventors used an eight bit register 151 that included four fixed bits and four bits for receiving key selection information. Each encryption key is one hundred and twenty eight bit long. It is noted that these lengths are provided as non-limiting examples.

The test enable circuit 170 includes a comparator 171 and an optional OR gate 172. One input of the comparator 171 is connected to the selected key register 158 and can receive the selected encryption key. Assuming that the key selection circuit 150 selected the right encryption key then the comparator 171 selects between this key to a key provided to its second input. The latter key can be provided via the test and debug unit, as represented by test and debug unit register 185.

If both keys match the comparator 171 sends a test approval signal that can be provided to an enable input of the test and debug unit 184.

5 According to an embodiment of the invention the output of the comparator 171 is sent to one input of the OR gate 172, while another input of the OR gate 172 received an inverted secured mode signal. The output of the OR gate 172 is connected to an enable input of the test and debug unit 184.

10 FIG. 3-7 and FIG. 9 illustrate a device booting sequence 300, according to an embodiment of the invention. Dashed lines illustrate the transferring of data or instructions between components.

15 Sequence 300 starts by an initial stage 310 of providing encrypted instructions and providing a device that is designed such as to limit and even prevent access to decrypted instructions.

20 Stage 310 is followed by stage 315 of resetting the device. Stage 315 can include resetting only a portion of the device, powering down the device of some of its components, a power failure, and the like.

Stage 315 is followed by stage 320 of retrieving and executing an initial boot code that conveniently is not encrypted.

25 Stage 320 is illustrated by FIG. 3. The processor 120 retrieves non-encrypted initial booting code from the third memory unit 180. The execution of the initial booting code initiates the decryption session.

30 Stage 320 is followed by stage 330 of preventing access to decrypted instructions that were decrypted prior to the resetting. This stage is required as the reset does not necessarily erase the content of various memories.

FIG. 4 illustrates stage 330. The second memory unit 130 or selected entries of said memory unit 120 are deleted. In addition, the instruction cache 122 or selected entries of the instruction cache are invalidated
5 by negating their valid bit. The selected entries usually store (or are suppose to store) decrypted instructions. It is noted that this stage can also include invalidating entries of the data cache 124.

Stage 330 is followed by stage 340 of receiving
10 encrypted instructions.

FIG. 5 illustrates stage 340. The processor 120 controls the downloading of encrypted instructions from the first integrated circuit 101, via interface 190, to the second memory unit 130. It is noted that the first
15 integrated circuit 102 can control the exchange in various manners, including a utilization of a DMA controller. During this downloading the device reads key selection information stored within the first integrated circuit 101.

Stage 340 is followed by stage 350 of decrypting and optionally de-hashing the decrypted instructions.

FIG. 6 illustrates stage 350. Device 100, and especially the encryption unit 140 perform de-hashing and decryption. The de-hashing is applied on each group of
25 instructions fetches by the decryption unit 140. If the de-hashing of a group of instructions is successful then these instructions are decrypted and sent, at their decrypted form, to the second memory unit 130. The processor 120 may control the decryption process, for
30 example by sending the key selection information retrieved from the first integrated circuit 101 to the key selection unit 150, by determining which group of

instructions is sent to the decryption unit 140, and where to decrypted instructions.

Stage 350 is followed by stage 360 of retrieving decrypted instructions and executing the decrypted
5 instructions. It is noted that the execution of some decrypted instructions can be executed at least in partially in parallel to the decryption of other encrypted instructions. FIG. 7 illustrates stage 360.

FIG. 7 illustrates the end of the booting session in
10 which the processor 120 retrieves decrypted instructions from the second memory unit 130 and executed them.

According to an embodiment of the invention the booting sequence further includes retrieving instructions from a fast interface 192, decrypting the instructions
15 and executing them. According to yet a further embodiment of the invention at least some of the decrypted instruction are associated with tasks other then booting the second integrated circuit 102.

FIG. 8 illustrates a method 200, according to an
20 embodiment of the invention.

Method 200 starts by stage 210 of providing encrypted instructions and providing a device that is designed such as to limit and even prevent access to decrypted instructions.

25 Stage 210 may include various sub-stages that are executed during various periods, including an integrated circuit design period, device 100 installation period, testing period and normal operational period.

Stage 210 may include designing the device such as
30 to limit access to a key database, limit access to fixed selection information, and the like, as well as designing interfaces that can be instructed from outside the device to directly access entries of memory units that may store

decrypted instructions. The limitation can include hardware limitations, such as not connecting various components to I/O interfaces.

5 Stage 210 may further include determining a fixed key selection information. Conveniently the determination is made by the manufacture of the second integrated circuit 102.

10 The fixed key information can then be provided to a client, such as another vendor or manufacturer that installs or utilizes the second integrated circuit in his product.

Stage 210 can also include providing a customer with at least one pair of encryption key and key selection information that corresponds to that encryption key.

15 Conveniently, stage 210 includes encrypting the instructions and optionally also hashing the decrypted instructions using a certain encryption key. The encrypted instructions are then stored at a first memory unit 110.

20 Stage 210 is followed by stage 230 of providing a default key before receiving the key selection information. The default key differs from the selected encryption key.

25 Stage 230 is followed by stage 240 of receiving key selection information.

30 Stage 240 is followed by stage 250 of receiving encrypted instructions. According to an embodiment of the invention the amount of receptions can be limited. Conveniently, after a reset occurred, only a single key selection information can be received reception after reset.

Stage 250 is followed by stage 260 of selecting a selected decryption key out of a key database in response

to fixed selection information and to the received key selection information.

Stage 260 is followed by stage 265 of de-hashing encrypted instructions and jumping to the stage 270 of
5 decrypting instructions if the de-hashing is successful.

If the de-hashing is not successful stage 265 can be followed by stage 266 of performing various actions such as sending an alert, issuing an interrupt, stopping the execution of code by processor 120, resetting the device,
10 and the like. Stage 266 can also be a part of a loop that allows certain amount of de-hashing failures without stopping the de-hashing and decryption sessions.

Stage 270 includes decrypting encrypted instructions using the selected decryption key. It is noted that both
15 the de-hashing and decrypting can be applied on groups of the encrypted instructions and that multiple iterations of stages 265 and 270 can be required before the whole encrypted instructions are decrypted successfully.

Stage 270 is followed by stage 290 of executing
20 decrypted instructions by a processor. Conveniently, this stage includes executing only instructions from predefined locations. It is noted that instructions that were decrypted in a decryption process that was controlled by a first processor can be executed by
25 another processor.

Method 200 may include stage 245 of preventing access to decrypted instructions stored in a device before a reset event. Stage 245 can be applied during the design stage of the second integrated circuit and may
30 include limiting the access of interfaces to various memory unit interfaces, and the like. Conveniently, stage 245 is also applied during a booting sequence of the

second integrated circuit 102 and can be applied as a part of the sequence of stages 230-295.

Conveniently, stage 245 includes invalidating instruction cache entries after reset. Conveniently,
5 stage 245 includes erasing memory unit entries. Conveniently, stage 245 includes allowing a testing unit to read an entry of a memory unit only after the testing unit wrote to that entry.

10 Stage 290 can be followed by stage 295 of selectively allowing testing or debugging of the device in response to a relationship between the selected decryption key and received key information. This stage can include receiving a request to test or debug the
15 second integrated circuit, waiting to receive a decryption key, and allowing the testing or debugging only if the provided decryption key matches the selected decryption key.

Either stages 290 or 295 can be followed by stage 230 once a reset occurred. The reset can result from a
20 shut down of device 100, from power failures, and the like.

Stage 295 can be followed by stage 290. If there is a need to decrypt additional instructions that were not previously decrypted then stage 290 can be followed by
25 stage 250.

Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed.
30 Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

WE CLAIM

1. A device (100) comprising a first memory unit (110)
5 adapted to store encrypted instructions, a processor
(120) adapted to execute decrypted instructions, a
second memory unit (130) accessible by the processor
(120), and a decryption unit (140),

characterized by comprising a key database (145) and
10 a key selection circuit (150), wherein the key selection
circuit (150) is adapted to select a selected decryption
key from the key database (145) for decrypting encrypted
instructions; and wherein the selection is responsive to
a fixed selection information stored within the
15 integrated circuit and to received key selection
information.

2. The device (100) according to claim 1 further
adapted to perform de-hashing of encrypted instructions
and in response to a result of the de-hashing determine
20 whether to decrypt the encrypted instructions.

3. The device (100) according to any claim of claims 1-
2 wherein the key selection circuit (150) is adapted to
limit an amount of receptions of key selection
information.

25 4. The device (100) according to any claim of claims
1-2 wherein the key selection circuit (150) is adapted to
allow a reception of one key selection information after
being reset.

5. The device (100) according to any claim of claims 1-
30 4 wherein the device is adapted to erase multiple entries
of the second memory unit (130) after reset.

6. The device (100) The device (100) according to any
claim of claims 1-5 wherein the processor (120) retrieves

information from an instruction cache (122) and wherein the device (100) is adapted to invalidate instruction cache entries after reset.

5 7. The device (100) according to any claim of claims 1-6 wherein the key selection circuit (150) is adapted to select a default key until receiving the key selection information.

10 8. The device (100) according to any claim of claims 1-7 wherein during test mode the test circuit (184) reads an entry of the second memory unit (130) only after previously writing to that entry.

9. The device (100) according to any claim of claims 1-8 wherein the processor (120) is adapted to execute only predefined instructions.

15 10. The device (100) according to any claim of claims 1-9 further comprising a test enable circuit (170) adapted to selectively facilitate testing or debugging of the processor (120) in response to a comparison between the selected decryption key and received key information.

20 11. The device (100) according to any claims out of claims 1-10 adapted to prevent access to the key database (145) and to the fixed selection information.

25 12. A method (200) comprising a stage of receiving (230) encrypted instructions; and executing (290) decrypted instructions by a processor;

characterized by receiving (240) key selection information; selecting (260) a selected decryption key out of a key database in response to fixed selection information and to the received key selection information; and decrypting (270) encrypted instructions using the selected decryption key.

30

13. The method (200) according to claim 12 further comprising de-hashing (265) encrypted instructions and

jumping to the stage of decrypting (270) if the de-hashing is successful.

14. The method (200) according to any claim of claims 12-13 further comprising limiting an amount of receptions
5 of key selection information.

15. The method (200) according to claim 14 wherein the limiting comprises allowing a single key selection information reception after reset.

16. The method (200) according to any claim of claims
10 12-13 further comprising preventing access to decrypted instructions stored in a device before a reset event.

17. The method (200) according to claim 16 wherein the preventing comprises invalidating instruction cache entries after reset.

18. The method (200) according to claim 16 wherein the preventing comprises erasing memory unit entries.
15

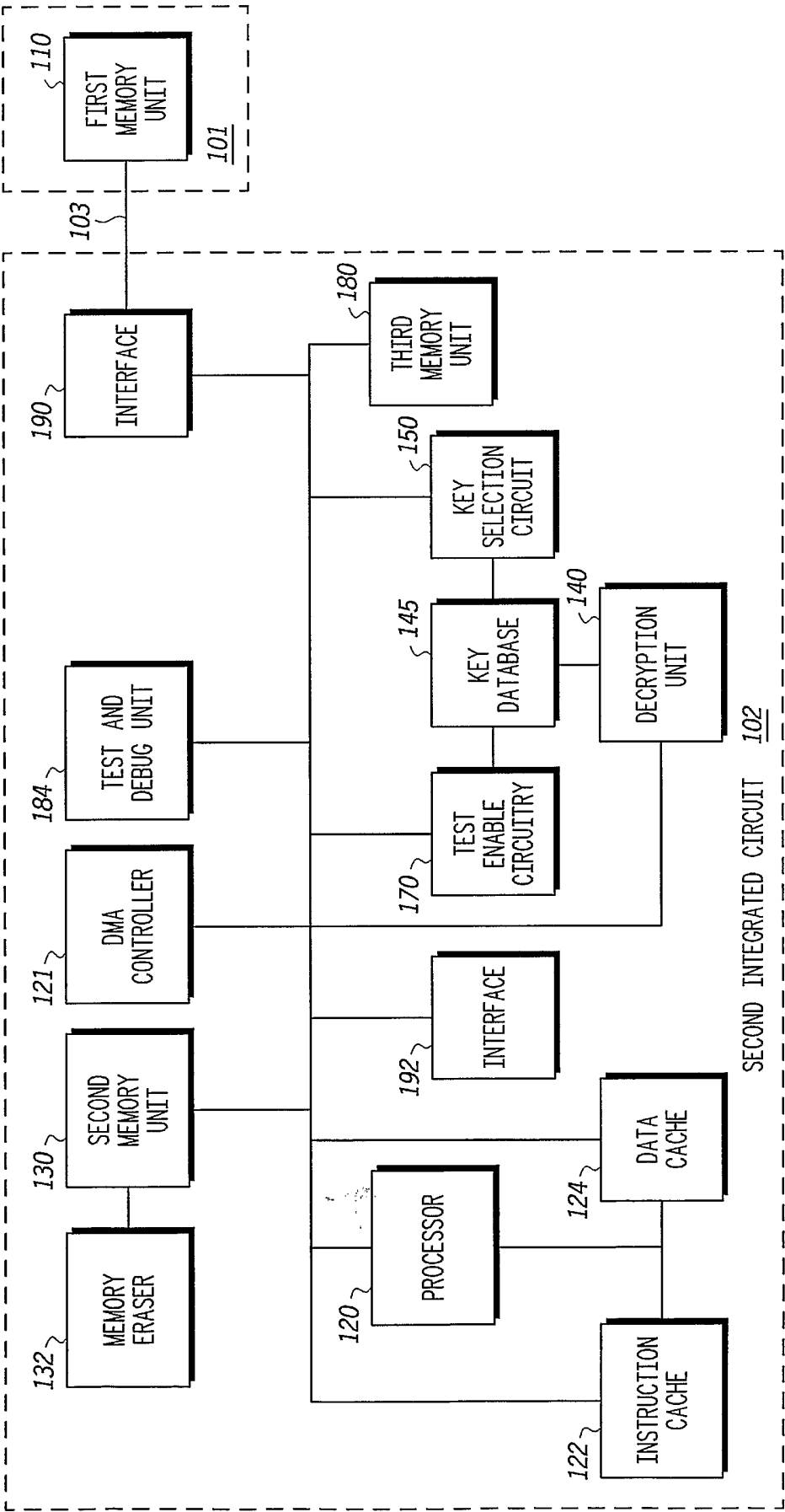
19. The method (200) according to claim 16 wherein the preventing comprises allowing a testing unit to read an entry of a memory unit only after the testing unit wrote
20 to that entry.

20. The method (200) according to any claim of claims 12-19 further comprising providing (230) a default key before receiving the key selection information.

21. The method (200) according to any claim of claims
25 12-20 wherein the stage of executing (290) comprises executing only instructions from predefined locations.

22. The method (200) according to any claim of claims 12-21 further comprising selectively allowing (295) testing or debugging in response to a relationship
30 between the selected decryption key and received key information.

23. The method (200) according to any claims out of claims 12-22 further comprising preventing access to the key database and to the fixed selection information.



100

FIG. 1

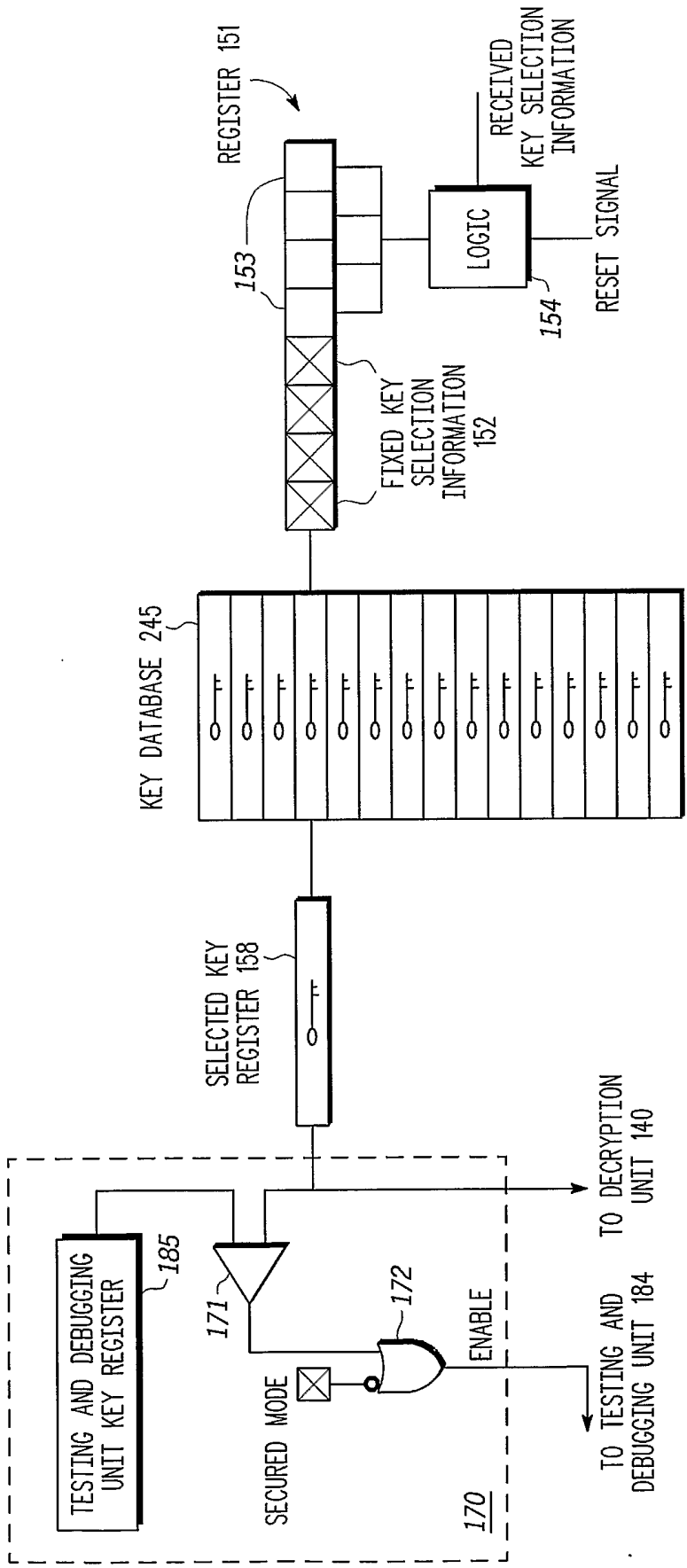
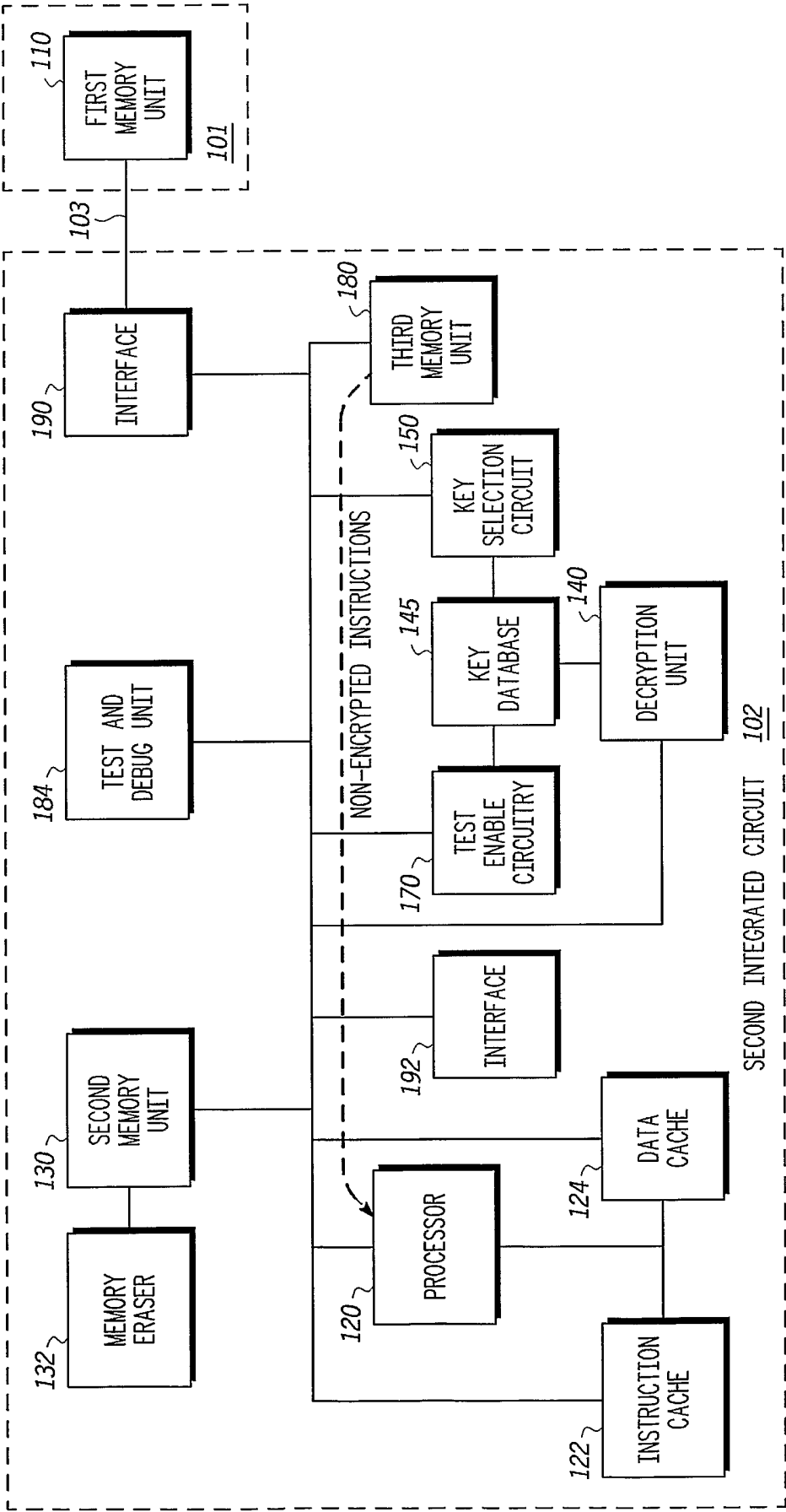
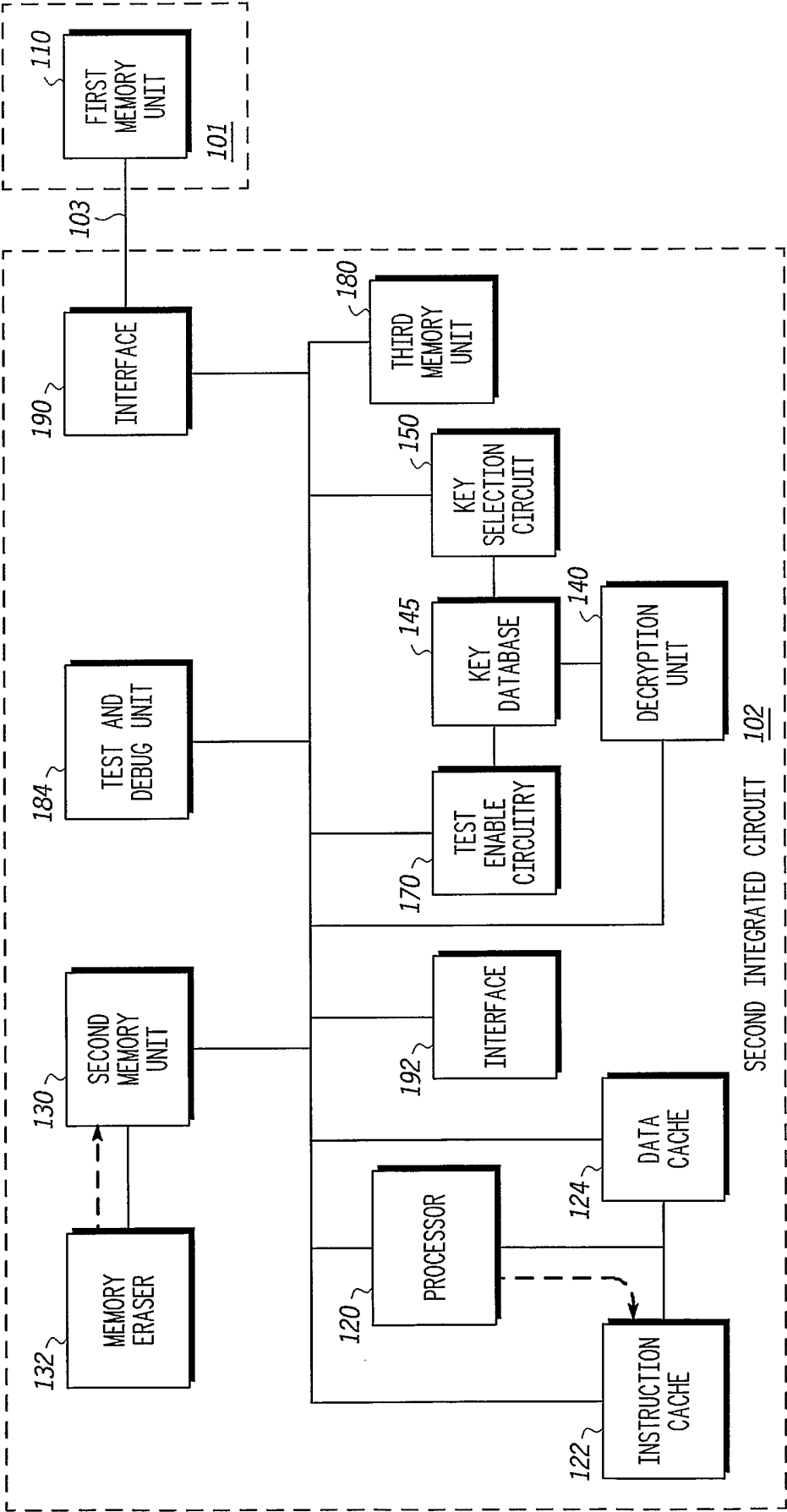


FIG. 2



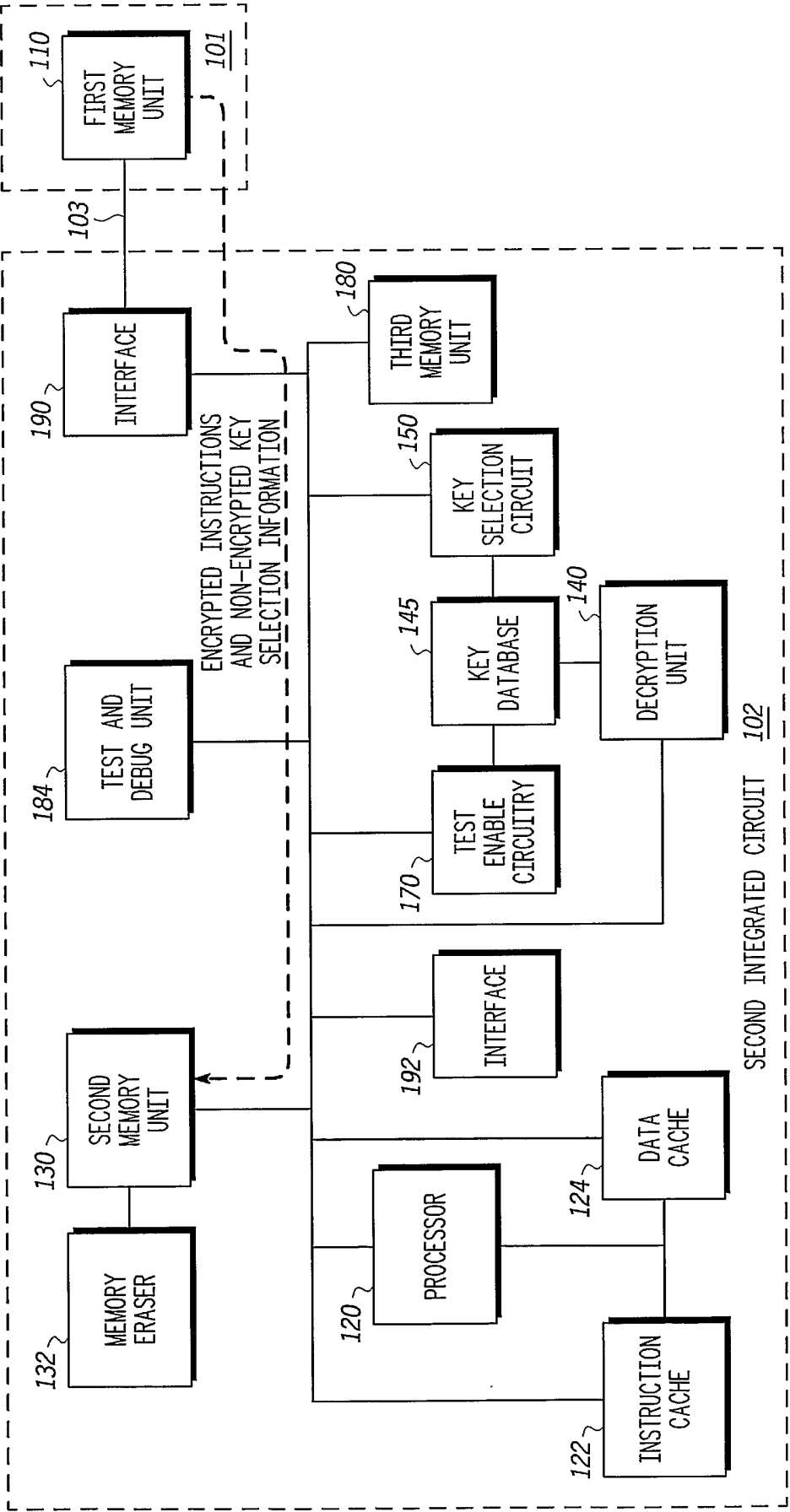
100

FIG. 3



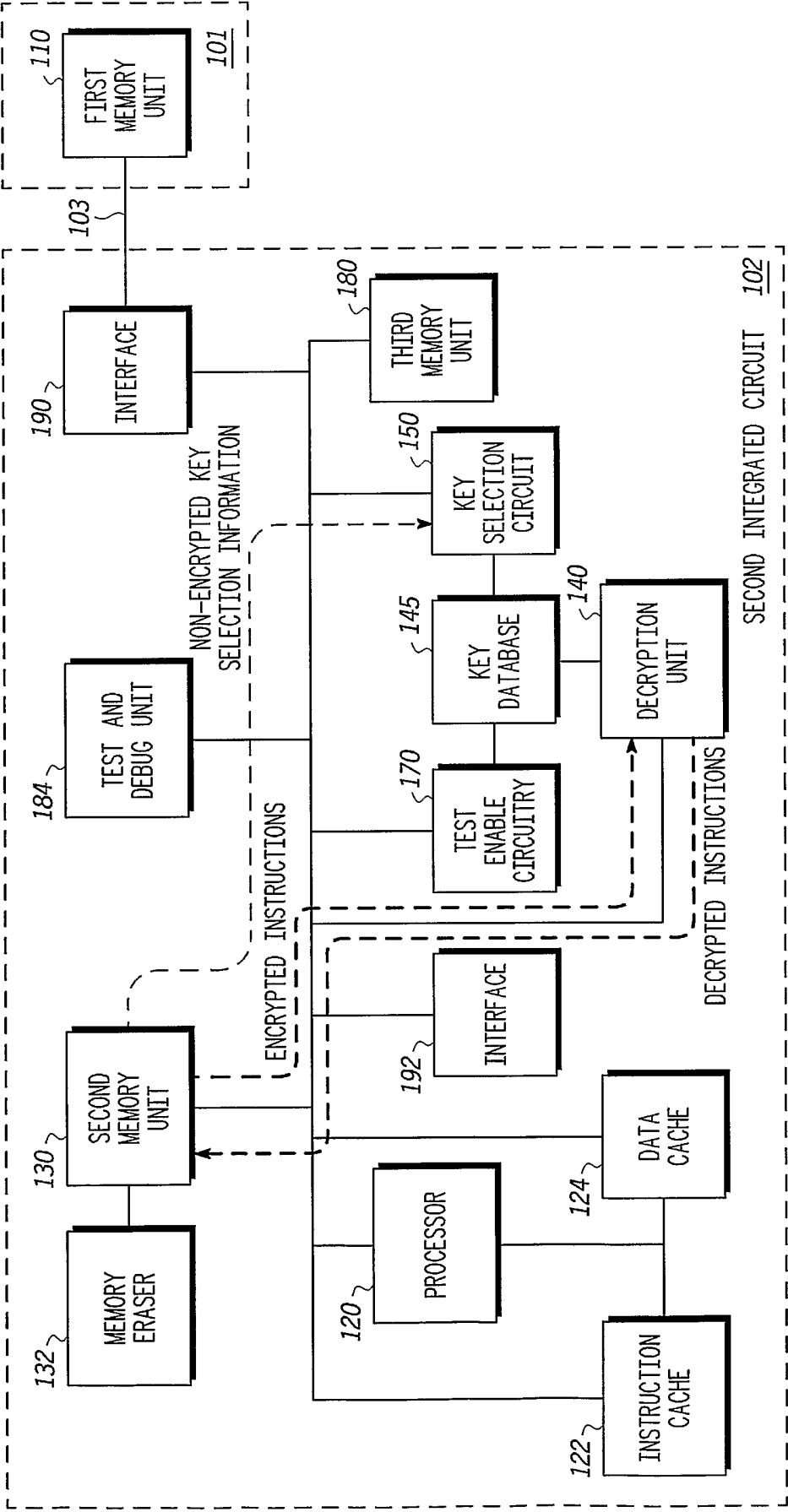
100

FIG. 4



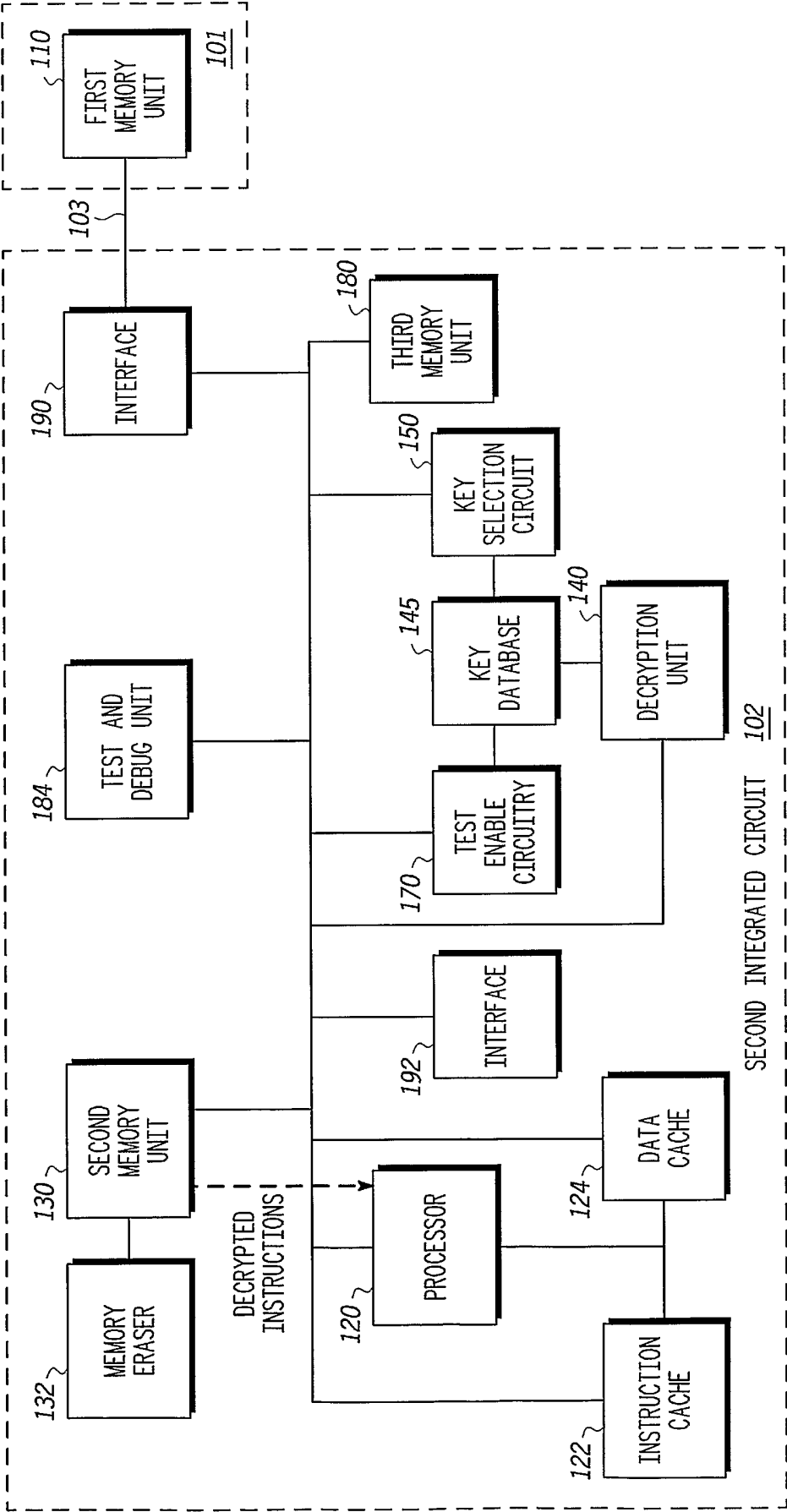
100

FIG. 5



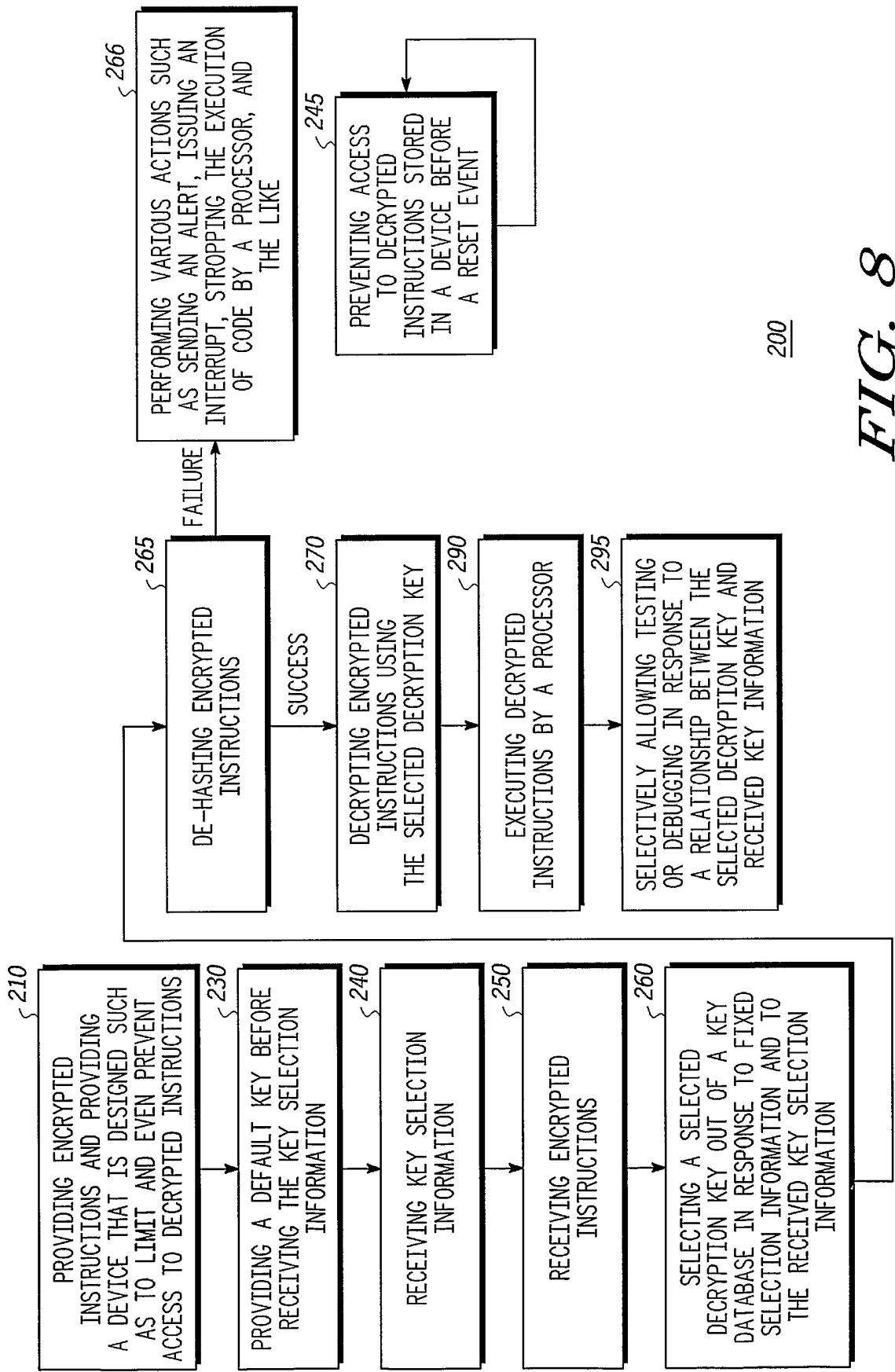
100

FIG. 6



100

FIG. 7



200

FIG. 8

9/9

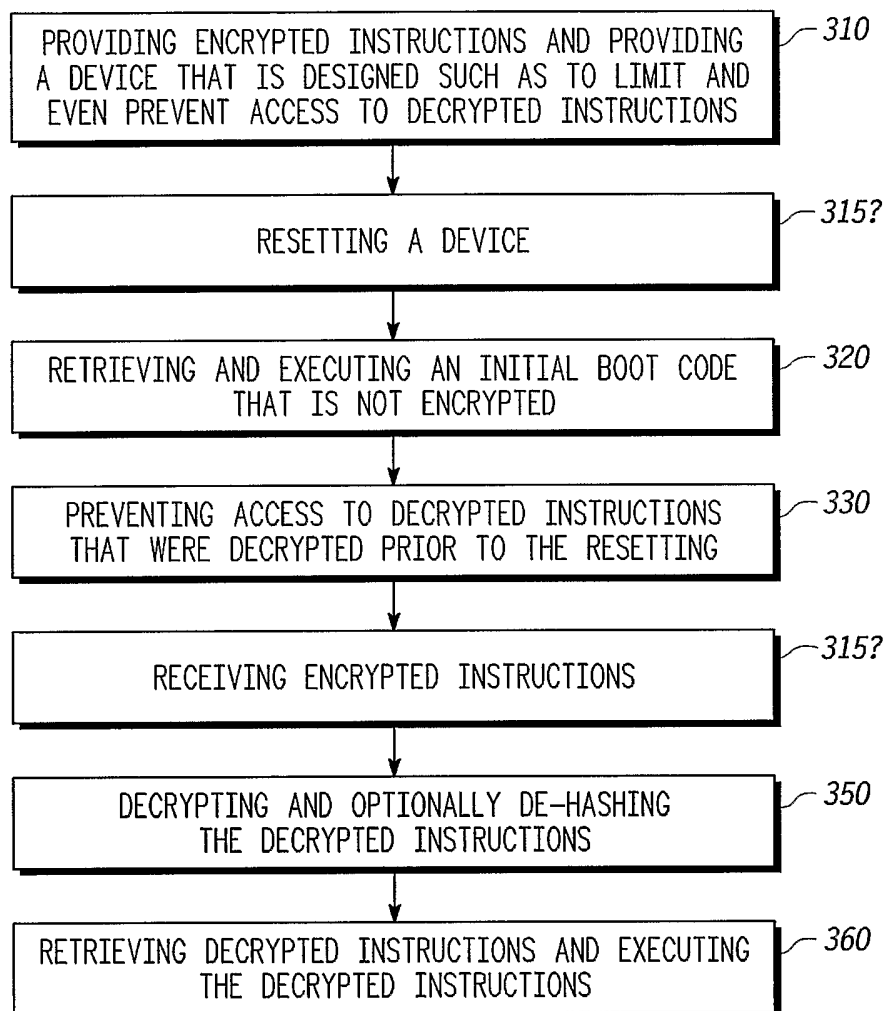


FIG. 9

INTERNATIONAL SEARCH REPORT

In ional application No
PCT/IB2005/052051

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/133574 A1 (CARONNI GERMANO ET AL) 17 July 2003 (2003-07-17) paragraph [0022] - paragraph [0027] figures 2,6,7A,7B,8	1,2, 7-13, 20-23
Y	----- US 6 304 970 B1 (BIZZARO MARIO ET AL) 16 October 2001 (2001-10-16) column 3, line 51 - line 53	3-6, 14-18
Y	----- US 5 515 540 A (GRIDER ET AL) 7 May 1996 (1996-05-07) column 18, line 52 - column 19, line 53	3,4,14, 15
Y	----- US 5 515 540 A (GRIDER ET AL) 7 May 1996 (1996-05-07) column 18, line 52 - column 19, line 53	5,6, 16-18
	----- -/--	

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

26 May 2006

Date of mailing of the international search report

02/06/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sigolo, A

INTERNATIONAL SEARCH REPORT

In ☐ national application No
PCT/IB2005/052051

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 298 242 A (SHARP KABUSHIKI KAISHA) 11 January 1989 (1989-01-11) column 1, line 36 - line 51 -----	5,6, 16-18
A	US 2005/105738 A1 (HASHIMOTO MIKIO) 19 May 2005 (2005-05-19) paragraph [0026] - paragraph [0035] paragraph [0065] - paragraph [0076] figures 1,2 -----	1,2, 11-13
A	US 4 874 902 A (HUANG ET AL) 17 October 1989 (1989-10-17) the whole document -----	1,2, 11-13
A	US 2005/091520 A1 (KHAN MOINUL H ET AL) 28 April 2005 (2005-04-28) paragraph [0025] - paragraph [0026] paragraph [0033] - paragraph [0035] -----	8,10,22
A	US 6 466 048 B1 (GOODMAN JAMES) 15 October 2002 (2002-10-15) the whole document -----	8,10,22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2005/052051

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1, 2, 11, 12, 13

Device and method for avoiding execution of corrupted instructions.

2. claims: 3, 4, 7, 8, 9, 10, 14, 15, 20, 21, 22

Device and method for preventing intrusion on a device.

3. claims: 5, 6, 16-19

Device and method for safely initializing a device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2005/052051

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2003133574	A1	17-07-2003	GB 2387937 A	29-10-2003
US 6304970	B1	16-10-2001	NONE	
US 5515540	A	07-05-1996	NONE	
EP 0298242	A	11-01-1989	CA 1305561 C	21-07-1992
			DE 3853321 D1	20-04-1995
			DE 3853321 T2	09-11-1995
			JP 1859222 C	27-07-1994
			JP 5064823 B	16-09-1993
			JP 63293664 A	30-11-1988
			US 4926388 A	15-05-1990
US 2005105738	A1	19-05-2005	JP 2005099984 A	14-04-2005
US 4874902	A	17-10-1989	NONE	
US 2005091520	A1	28-04-2005	WO 2005043301 A2	12-05-2005
US 6466048	B1	15-10-2002	US 2002175698 A1	28-11-2002