



(51) International Patent Classification:

G06F 21/57 (2013.01) *G06F 9/44* (2018.01)

(21) International Application Number:

PCT/US2017/029129

(22) International Filing Date:

24 April 2017 (24.04.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventors: **STEWART, Christopher H.**; 11445 Compaq Center Dr W, Houston, Texas 77070 (US). **ANBAZHAGAN, Baraneedharan**; 11445 Compaq Center Dr W,

Houston, Texas 77070 (US). **WANG, Lan**; 9600 West Gulf Bank Road, Houston, Texas 77040 (US).

(74) Agent: **MAISAMI, Ceyda A.** et al.; HP INC., 3390 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: DISPLAYING A BIOS UPDATE PROGRESS

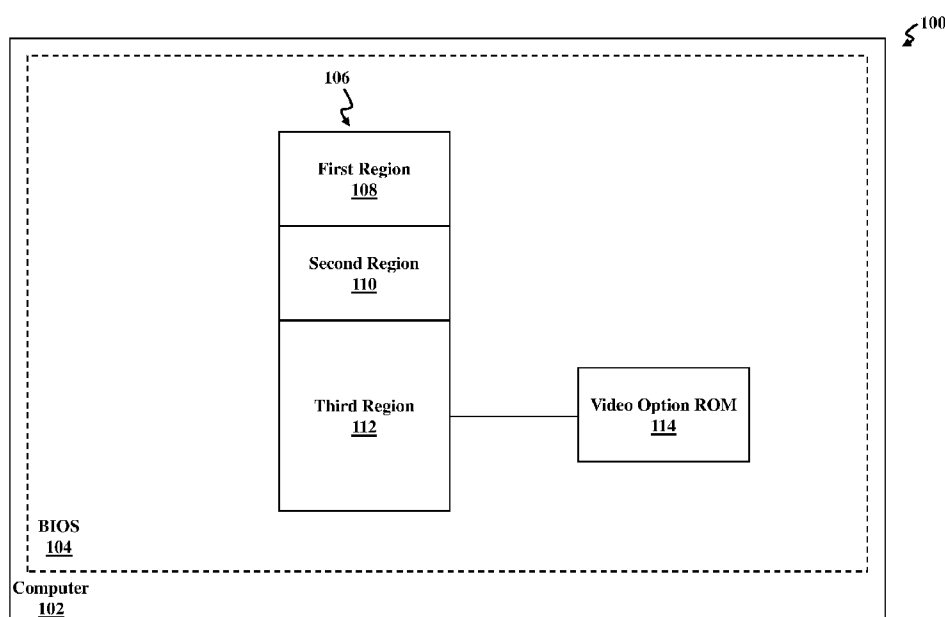


FIG. 1

(57) Abstract: The update progress of a basic input/output system (BIOS) is displayed on a display screen. A first chipset lock is applied to a first region of a shared serial peripheral interface (SPI) chip of the BIOS of a computer system containing a first program of instructions. A system management memory mode lock is applied to a second and a third region of the shared SPI chip containing a second and third programs of instructions respectively. The second program of instructions is updated, and control of the BIOS is transferred to the updated second program of instructions. The updated second program of instructions updates the first program of instructions. The BIOS update progress visual is displayed on the display screen of the computer system while updating the first program of instructions.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- *as to the identity of the inventor (Rule 4.17(i))*
- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

- *with international search report (Art. 21(3))*

DISPLAYING A BIOS UPDATE PROGRESS

BACKGROUND

[0001] The Basic Input/Output System (BIOS) may include computer program instructions that initialize the input and output operations of the computer system. The BIOS may take control of the computer system at the beginning stages of the computer system startup. The computer program instructions in the BIOS may need to be updated to the latest release by the computer system vendor. While performing such updates, the BIOS program instructions should be protected from an untrusted source.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. 1 is a schematic diagram illustrating a BIOS system, according to an example herein;

[0003] FIG. 2 is a schematic diagram illustrating an update process of a BIOS system, according to an example herein;

[0004] FIG. 3 is a schematic diagram illustrating an update process of a BIOS system, according to an example herein;

[0005] FIG. 4 is a flow diagram illustrating a method for updating a BIOS system, according to an example herein; and

[0006] FIG. 5 illustrates a schematic diagram of a computer system used in accordance with the examples herein.

DETAILED DESCRIPTION

[0007] The examples herein provide a secure BIOS update, while displaying an update progress video on a screen for a user of the computer system. This provides a user-friendly solution and also provides the required security during the BIOS update process. The examples herein overcome the issue of a lack of sufficient updates regarding the progress of the BIOS update and thereby reduce

the possibility that a user may reboot the computer system while the update is taking place, which overcomes potential failures of the BIOS update process.

[0008] FIG. 1 is a schematic diagram illustrating a system 100, according to an example herein. The system 100 may include a shared serial peripheral interface (SPI) chip 106 of a BIOS 104 of a computer 102. The BIOS 104 includes a first region 108 configured to store a first copy of a pre-extensible firmware interface (PEI) program of instructions. A second region 110 of the BIOS 104 may be configured to store a second copy of the PEI program of instructions. A third region 112 may be configured to store a driver execution environment (DXE) program of instructions.

[0009] The DXE program of instructions may include more features compared to the PEI program of instructions. For example, the DXE program can have access to the drivers of other components of the computer 102, such as a graphical card. In an example herein, the DXE program of instructions may display a progress of an update of the first PEI program of instructions, using a video option read-only memory (ROM) 114 and the DXE program of instructions. The PEI program of instructions may not have the capability of using the video option ROM 114, or the PEI program of instructions may have the capability of using a video option ROM that lacks the richness of display features available to the DXE program of instructions.

[0010] The shared SPI chip 106 may be configured to apply a first chipset lock to the first region 108, and apply a system management memory mode (SMM) lock to the second and third regions 110 and 112. In an example herein, when the chipset lock is applied to a region of a chip 106, it will prevent any write to that region of the chip 106 until the chip 106 is reset. Therefore, in an example herein, when the first chipset lock is applied to the first region 108 of the shared SPI chip 106, nothing can be written to the first region 108 until the shared SPI chip 106 is reset. In an example, resetting the SPI chip 106 includes electronically disconnecting the chip 106 from a power source, and then reconnecting the chip 106 to the power source.

[0011] In an example herein, when the SMM lock is applied to a region of a chip 106, only a special software of the operating system of the computer system 102 may write data to that region of the chip 106. In an example herein, this special software is isolated from the rest of the operating system of the computer system 102.

[0012] FIG. 2, with reference to FIG. 1, is a schematic diagram illustrating a system 200, according to an example herein. The BIOS 104 may be configured to update the second copy of the PEI program of instructions and execute the updated second copy of the PEI program of instructions. In an example herein, the BIOS 104 may be configured to apply a second chipset lock to the second region 110 of the shared SPI chip 106. The BIOS 104 may apply the second chipset lock after executing the updated second copy of the PEI program of instructions.

[0013] In an example herein, the BIOS 104 may be configured to generate a random number shared secret key 116, and transmit the random number shared secret key 116 to the third region 112 of the shared SPI chip 106. In an example herein, the random number shared secret key 116 is a set of digital values. The BIOS 104 may store the random number shared secret key 116 in a system management random access memory (SMRAM) 118. In an example herein, the SMRAM 118 is isolated from a main random access memory (RAM) 130 of the computer system 102. The SMRAM 102 may also store the special software of the operating system of the computer system 102 that is configured to write data to the SMM locked regions of the shared SPI chip 106.

[0014] In an example herein, after storing the random number shared secret key 116 in the SMRAM 118, the BIOS 104 may securely delete a received copy of the random shared secret key 116 by the third region 112 of the shared SPI chip 106. Securely deleting the received copy of the shared secret key 116 by the third region 112 of the shared SPI chip 106 may include digitally shredding the received copy of the shared secret key 116 by zeroing out the received copy of the shared secret key 116 using a secure zero memory operation. In an example herein, the zero memory operation is considered secure if it meets two requirements as set

forth by the United States National Institute of Standards and Technology (NIST). First, the memory location that is being securely zeroed out is to be assigned several different values in succession, and then is assigned the value of “zero.” Second, the secure zero memory operation is to be written in a language-specific manner such that a compiler does not need to further optimize the secure zero memory operation.

[0015] In an example herein, the random number shared secret key 116 may be sent from the second region 110 to the third region 112 via a hand-off block (HOB) 202. The HOB 202 is a data structure used for transmitting data between the PEI and DXE program of instructions.

[0016] FIG. 3, with reference to FIGS. 1 and 2, is a schematic diagram illustrating a system 300, according to an example herein. The BIOS 104 may further include an embedded controller (EC) 120 and a private SPI chip 119 electronically coupled to the embedded controller 120. In an example herein, the private SPI chip 119 may be electronically isolated from any other component of the BIOS 104, except the embedded controller 120.

[0017] In an example herein, the BIOS 104 may be set to transmit the random number shared secret key 116 to the private SPI chip 119. The BIOS 104 may transmit the random number shared secret key 116 to the private SPI chip 119 using the embedded controller 120. After transmitting the random number shared secret key 116 to the private SPI chip 119, the BIOS 104 may seal a trusted application program interface (API) on the embedded controller 120 to secure the random number shared secret key 116. In an example herein, the BIOS 104 may seal the API on the embedded controller using SMM lock. In an example, any other mechanism may be used for sealing the API, provided the mechanism renders the specific location of the private SPI chip 119 which is controlled by the embedded controller 120, immutable until the BIOS power is reset or a demonstrated trusted caller requests that the seal be removed for a temporary duration. In an example, the demonstrated trusted caller is a caller with knowledge of the shared secret key 116.

[0018] In an example herein, the BIOS 104 may be set to securely transfer the updated second copy of the PEI program of instructions from the second region 110 to the private SPI chip 119. The BIOS 104 may hash the updated second copy of the PEI program of instructions using the random number shared secret key 116 before transferring to the private SPI 119. In an example herein, to establish trust with the embedded controller 120, the BIOS 104 may use a keyed-hash message authentication code (HMAC) process, such as Secure Hash Algorithm 2 (SHA-2) for securely transferring the updated second copy of the PEI program of instructions from the second region 110 to the private SPI chip 119, using the random number shared secret key 116. In an example herein, the BIOS 104 may securely transfer the updated second copy of the PEI program of instructions from the second region 110 to the private SPI chip 119, one block at a time, using HMAC on each block.

[0019] In an example herein, the BIOS 104 may display the update progress of copying the PEI program of instructions from the second region 110 to the private SPI chip 119, using the video option ROM 114, while securely transferring the updated second copy of the PEI program of instructions. In an example herein, the video option ROM 114 may be communicatively coupled to a display screen 122 of the computer 102. The update progress may be displayed on the display screen 122 using, for example, any of a progress bar, textual update, or a simulated image or video sequence of the BIOS updating process.

[0020] In an example herein, the embedded controller 120 may be configured to verify the authentication of the hashed updated second copy of the PEI program of instructions using the random number shared secret key 116 that is securely stored in the private SPI chip 119. In an example, the hashed version of the second copy of the PEI program of instructions is divided into multiple blocks of data and is sent to the private SPI chip 119 of the embedded controller 120 one block at a time. A block of data may be of any size supported by a communication mechanism 310 between the shared SPI chip 106 and the private SPI chip 119 of the embedded controller 120. In an example, the authentication of each individual

block is verified by the embedded controller 120. In another example, the individual blocks are rearranged in succession to reconstruct the transmitted hashed version of the second copy of the PEI program of instructions, and the authentication of the received data is also verified after it is reconstructed. The verifications by the embedded controller 120 may be performed using the HMAC process, as described above. If the embedded controller 120 verifies the authentication, the embedded controller 120 may extract the updated second copy of the PEI program of instructions using the random number shared secret key 116.

[0021] After the embedded controller 120 verifies the authentication of the hashed updated second copy of the PEI program of instructions, the BIOS 104 may reset the shared SPI chip 106. Resetting the shared SPI chip 106 removes the first chipset lock on the first region 108 of the shared SPI chip 106.

[0022] In an example herein, after removing the first chipset lock from the first region 108 of the shared SPI chip 106, the embedded controller 120 transfers the updated second copy of the PEI program of instructions to the first region 108 of the shared SPI chip 106. After transferring the updated second copy of the PEI program of instructions to the first region 108 of the shared SPI chip 106, the updated program of instructions in the first region 108 is executed.

[0023] FIG. 4, with reference to FIGS. 1 through 3, is a flowchart illustrating a method 400 according to an embodiment herein. At block 404, the method 400 may apply a first chipset lock to a first region 108 of a shared SPI chip 106 of a BIOS 104 of a computer system 102. The first region 108 may contain a first program of instructions.

[0024] At block 404, the method 400 may apply a system management memory mode lock to a second region 110 and a third region 112 of the shared SPI chip 106, wherein the second region 110 contains a second program of instructions, and the third region 112 contains a third program of instructions. At block 406, the method 400 may update the second program of instructions.

[0025] At block 408, the method 400 may transfer control of the BIOS 104 to

the updated second program of instructions. At block 410, the method 400 may update the first program of instructions using the updated second program of instructions. At block 412, the method 400 may display a BIOS update progress visual on a display screen 122 of the computer system 102 while updating the first program of instructions.

[0026] In an example herein, the method 400 may further include executing the updated second program of instructions, and applying a second chipset lock to the second region 110 of the shared SPI chip 106. In another example herein, the method 400 may further include generating a random number shared secret key 116, transmitting the random number shared secret key 116 to the third region 112 of the shared SPI chip 106, storing the random number shared secret key 116 in a system management random access memory (SMRAM) 118 of the computer system 102, and securely deleting a received copy of the random shared secret key 116 by the third region 112 of the shared SPI chip 106.

[0027] In another example herein, the method 400 may further include transmitting the random number shared secret key 116 to an embedded controller 120 of the BIOS 104, and securing the random number shared secret key 116 by sealing a trusted application program interface on the embedded controller 120 to prevent the random number shared secret key 116 from being changed by another computer system.

[0028] In another example herein, the method 400 may further include hashing the updated second program of instructions using the random number shared secret key 116, securely transferring the updated second program of instructions from the second region 110 to a private SPI chip 119, wherein the private SPI chip 119 may be controlled by the embedded controller 120, and displaying the BIOS update progress visual on the display screen 122 while securely transferring the updated second program of instructions.

[0029] In another example herein, the method 400 may include verifying the authentication of the hashed updated second program of instructions using the random number shared secret key 116, and resetting the BIOS 104 when the

authentication of the hashed updated second program of instructions is verified.

[0030] In another example herein, the method 400 may include removing the first chipset lock from the first region 108 of the shared SPI chip 106, and transferring the updated second program of instructions to the first region 108 of the shared SPI chip 106.

[0031] Various examples herein can include both hardware and software elements. The examples that are implemented in software include but are not limited to, firmware, resident software, microcode, etc. Other examples may include a computer program product configured to include a pre-configured set of instructions, which when performed, can result in actions as stated in conjunction with the methods described above. In an example, the pre-configured set of instructions can be stored on a tangible non-transitory computer readable medium or a program storage device containing software code.

[0032] A representative hardware environment for practicing the examples herein is depicted in FIG. 5, with reference to FIGS. 1 through 4. This schematic drawing illustrates a hardware configuration of the information handling/computer system 102 according to an example. The computer system 102 may include at least one processor or central processing unit (CPU) 1010. The CPUs 1010 are interconnected via system bus 1012 to various memory devices 1014, 1016 such as a random access memory (RAM) 1014 and a read-only memory (ROM) 1016. The memory devices 1014, 1016 can include local memory employed during actual execution of the program code, bulk storage, and cache memories which provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution. An I/O adapter 1018 can connect to peripheral devices, such as disk units 1011 and storage drives 1013, or other program storage devices that are readable by the computer system 102. The computer system 102 may further include a user interface adapter 1019 that may connect to a keyboard 1015, mouse 1017, speaker 1024, microphone 1022, and/or other user interface devices such as a touch screen device (not shown) to the bus 1012 to gather user input. Additionally, a communication

adapter 1020 connects the bus 1012 to a data processing network 1025, and a display adapter 1021 connects the bus 1012 to a display device 1023, which provides a graphical user interface (GUI) 1029 for a user to interact with. The display device 1023 may include the display screen 122. Further, a transceiver 1026, a signal comparator 1027, and a signal converter 1028 may be connected to the bus 1012 for processing, transmission, receipt, comparison, and conversion of electric or electronic signals, respectively.

[0033] The computer system 102 may further include the BIOS 104 including a storage medium 1030. In an example herein, the storage medium 1030 may be a non-transitory machine-readable storage medium storing instructions that upon execution cause the BIOS 104 to apply a first chipset lock to a first pre-extensible firmware interface initialization (PEI) region 108 of a shared serial peripheral interface (SPI) chip 106 of the basic input/output system (BIOS) 104 of the computer system 102.

[0034] The stored instructions, upon execution, may further cause the BIOS 104 to update a program of instructions stored in a second PEI region 110 of the shared SPI chip 106, execute the updated program of instructions from the second PEI region 110, and generate a random number shared secret key 116.

[0035] The stored instructions, upon execution, may further cause the BIOS 104 to apply a second chipset lock to the second PEI region 110, and transmit the updated program of instructions to a driver execution environment (DXE) region 112 of the shared SPI chip 106.

[0036] The stored instructions, upon execution, may further cause the BIOS 104 to apply a third chipset lock to the DXE region 112 of the shared SPI chip 106, and transfer the random number shared secret key 116 to the DXE region 112 via a HOB 202, which may include a format readable by the DXE region 112.

[0037] The stored instructions, upon execution, may further cause the BIOS 104 to store the random number shared secret key 116 in a SMRAM 118, and transmit the random number shared secret key 116 to an embedded controller 120 of the BIOS 104.

[0038] The stored instructions, upon execution, may further cause the BIOS 104 to hash the updated program of instructions using the random number shared secret key 116, and securely transfer the updated program of instructions from the DXE region 112 to a private SPI chip 119 wherein the private SPI chip 119 may be controlled by the embedded controller 120.

[0039] In an example, after the BIOS 104 stores the random number shared secret key 116 in the SMRAM 118, and securely transfers the updated program of instructions from the DXE region 112 to the private SPI chip 119, the BIOS 104 may remove the random number shared secret key 116 from the DXE region 112 by a secure zero memory operation. In an example, after the BIOS 104 securely transfers the updated program of instructions from the DXE region 112 to the private SPI chip 119, the shared SPI chip 106 is rebooted, and following the reboot the random number shared secret key 116 is securely removed from the DXE region 112. However, the BIOS 104 may retain the random number shared secret key 116 in the DXE region 112 while transmission of the updated program of instructions from the DXE region 112 to the private SPI chip 119 is in progress.

[0040] The stored instructions, upon execution, may further cause the BIOS 104 to present an update progress message to a display screen 122, using a video option read-only memory (ROM) 114, while securely transferring the updated program of instructions from the DXE region 112 of the shared SPI chip 106 to the private SPI chip 119, regardless whether the video option ROM 114 is trusted.

[0041] In an example herein, the non-transitory machine-readable storage medium 1030 may store instructions that upon execution cause the BIOS 104 to verify authentication of the hashed updated program of instructions at the private SPI chip 106 using the random number shared secret key 116, reset the shared SPI chip 106 when the authentication of the hashed updated program of instructions is verified, remove the first chipset lock from the first PEI region 108 of the shared SPI chip 106, and transfer the updated program of instructions to the first PEI region 108 of the shared SPI chip 106.

[0042] The present disclosure has been shown and described with reference

to the foregoing exemplary implementations. Although specific examples have been illustrated and described herein it is manifestly intended that the scope of the claimed subject matter be limited only by the following claims and equivalents thereof. It is to be understood, however, that other forms, details, and examples may be made without departing from the spirit and scope of the disclosure that is defined in the following claims.

CLAIMS

What is claimed is:

1. A method comprising:
 - applying a first chipset lock to a first region of a shared serial peripheral interface (SPI) chip of a basic input/output system (BIOS) of a computer system, wherein the first region contains a first program of instructions;
 - applying a system management memory mode lock to a second region and a third region of the shared SPI chip, wherein the second region contains a second program of instructions, and the third region contains a third program of instructions;
 - updating the second program of instructions;
 - transferring control of the BIOS to the updated second program of instructions;
 - updating the first program of instructions using the updated second program of instructions; and
 - displaying a BIOS update progress visual on a display screen of the computer system while updating the first program of instructions.
2. The method of claim 1, comprising:
 - executing the updated second program of instructions; and
 - applying a second chipset lock to the second region of the shared SPI chip.
3. The method of claim 1, comprising:
 - generating a random number shared secret key;
 - transmitting the random number shared secret key to the third region of the shared SPI chip;
 - storing the random number shared secret key in a system management random access memory (SMRAM) of the computer system; and
 - securely deleting a received copy of the random shared secret key by the third region of the shared SPI chip.

4. The method of claim 3, comprising:
 - transmitting the random number shared secret key to an embedded controller of the BIOS; and
 - securing the random number shared secret key by sealing a trusted application program interface on the embedded controller to prevent the random number shared secret key from being changed by another computer system.
5. The method of claim 4, comprising:
 - hashing the updated second program of instructions using the random number shared secret key;
 - securely transferring the updated second program of instructions from the second region to a private SPI chip, wherein the private SPI chip is controlled by the embedded controller; and
 - displaying the BIOS update progress visual while securely transferring the updated second program of instructions.
6. The method of claim 5, comprising:
 - verifying authentication of the hashed updated second program of instructions using the random number shared secret key; and
 - resetting the BIOS when the authentication of the hashed updated second program of instructions is verified.
7. The method of claim 2, comprising:
 - removing the first chipset lock from the first region of the shared SPI chip;
 - and
 - transferring the updated second program of instructions to the first region of the shared SPI chip.
8. A non-transitory machine-readable storage medium storing instructions that

upon execution cause an electronic device to:

- apply a first chipset lock to a first pre-extensible firmware interface initialization (PEI) region of a shared serial peripheral interface (SPI) chip of a basic input/output system (BIOS) of a computer;

- update a program of instructions stored in a second PEI region of the shared SPI chip;

- execute the updated program of instructions from the second PEI region;

- generate a random number shared secret key;

- apply a second chipset lock to the second PEI region;

- transmit the updated program of instructions to a driver execution environment (DXE) region of the shared SPI chip;

- apply a third chipset lock to the DXE region of the shared SPI chip;

- transfer the random number shared secret key to the DXE region via a hand-off block (HOB), wherein the HOB comprises a format readable by the DXE region;

- store the random number shared secret key in a system management random access memory (SMRAM);

- transmit the random number shared secret key to an embedded controller of the BIOS;

- hash the updated program of instructions using the random number shared secret key;

- securely transfer the updated program of instructions from the DXE region to a private SPI chip, wherein the private SPI chip is controlled by the embedded controller; and

- present an update progress message to a display screen, using a video option read-only memory (ROM), while securely transferring the updated program of instructions from the DXE region of the shared SPI chip to the private SPI chip, regardless whether the video option ROM is trusted.

9. The non-transitory machine-readable storage medium of claim 8, wherein

the instructions upon execution cause the electronic device to:

- verify authentication of the hashed updated program of instructions at the private SPI chip using the random number shared secret key;
- reset the shared SPI chip when the authentication of the hashed updated program of instructions is verified;
- remove the first chipset lock from the first PEI region of the shared SPI chip;
- and
- transfer the updated program of instructions to the first PEI region of the shared SPI chip.

10. A system comprising:

a shared serial peripheral interface (SPI) chip of a basic input/output system (BIOS) of a computer, comprising:

- a first region configured to store a first copy of pre-extensible firmware interface (PEI) program of instructions;
 - a second region configured to store a second copy of PEI program of instructions; and
 - a third region configure to:
 - store a driver execution environment (DXE) program of instructions; and
 - display a progress of an update of the first PEI program of instructions, using a video option read-only memory (ROM) and the DXE program of instructions;
- wherein the shared SPI chip is configured to apply a first chipset lock to the first region, and apply a system management memory mode lock to the second and third regions.

11. The system of claim 10, wherein the BIOS is set to:

- update the second copy of the PEI program of instructions;
- execute the updated second copy of the PEI program of instructions;

apply a second chipset lock to the second region of the shared SPI chip;
generate a random number shared secret key;
transmit the random number shared secret key to the third region of the shared SPI chip; and
store the random number shared secret key in a system management random access memory.

12. The system of claim 11, comprising:
an embedded controller of the BIOS; and
a private SPI chip electronically coupled to the embedded controller;
wherein the BIOS is set to:
transmit the random number shared secret key to the private SPI chip; and

seal a trusted application program interface on the embedded controller to secure the random number shared secret key.

13. The system of claim 12, wherein the BIOS is set to:
securely transfer the updated second copy of the PEI program of instructions from the second region to the private SPI chip;
hash the updated second copy of the PEI program of instructions using the random number shared secret key before transferring to the private SPI; and
display the update progress, using the video option ROM, while securely transferring the updated second copy of the PEI program of instructions.

14. The system of claim 13, wherein the embedded controller is set to:
verify authentication of the hashed updated second copy of the PEI program of instructions using the random number shared secret key from the private SPI chip; and
reset the shared SPI chip when the authentication of the hashed updated second copy of the PEI program of instructions is verified.

15. The system of claim 14, wherein the embedded controller is set to:
remove the first chipset lock from the first region of the shared SPI chip; and
transfer the updated second copy of the PEI program of instructions to the
first region of the shared SPI chip.

100

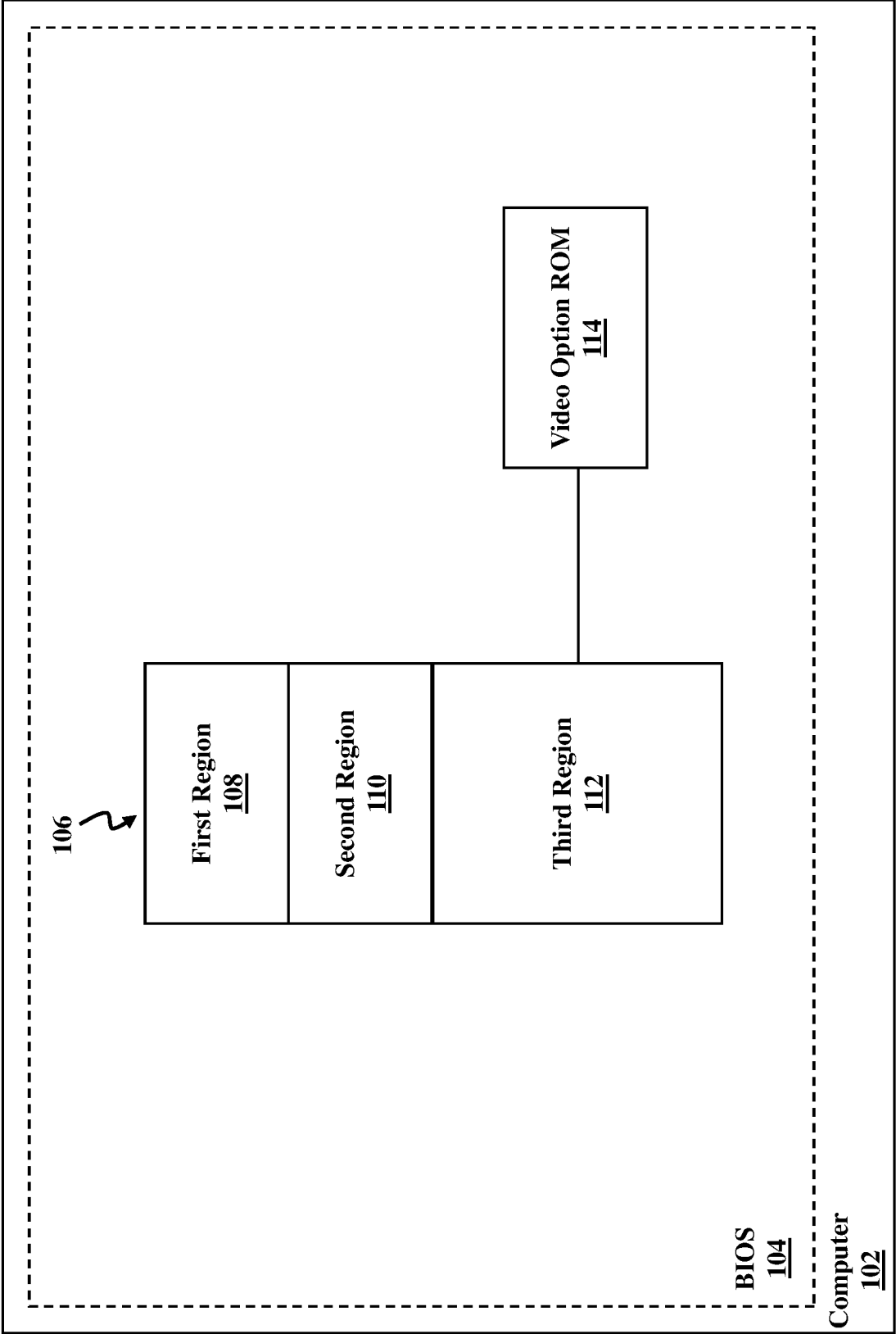


FIG. 1

200 ↗

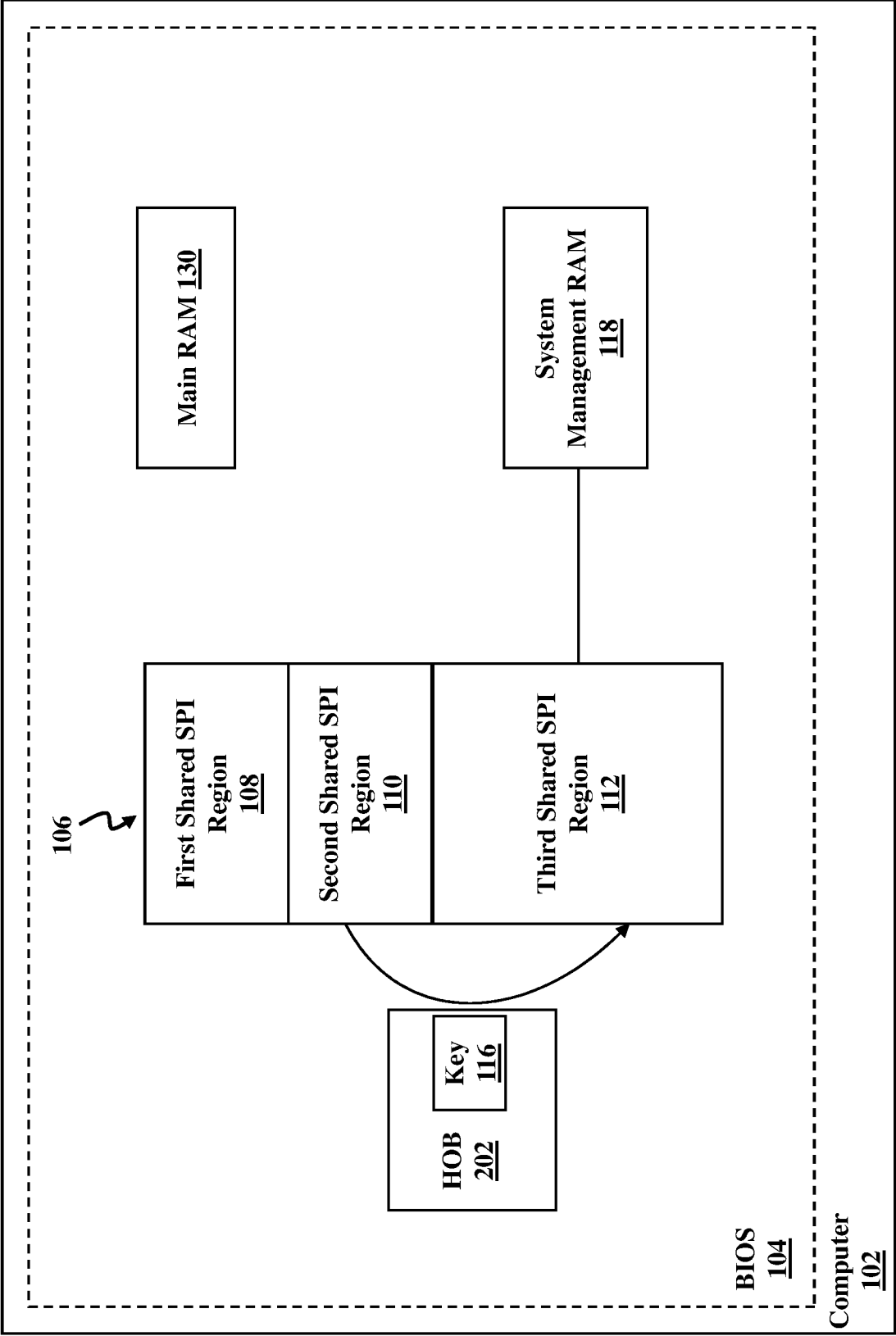


FIG. 2

300 ↗

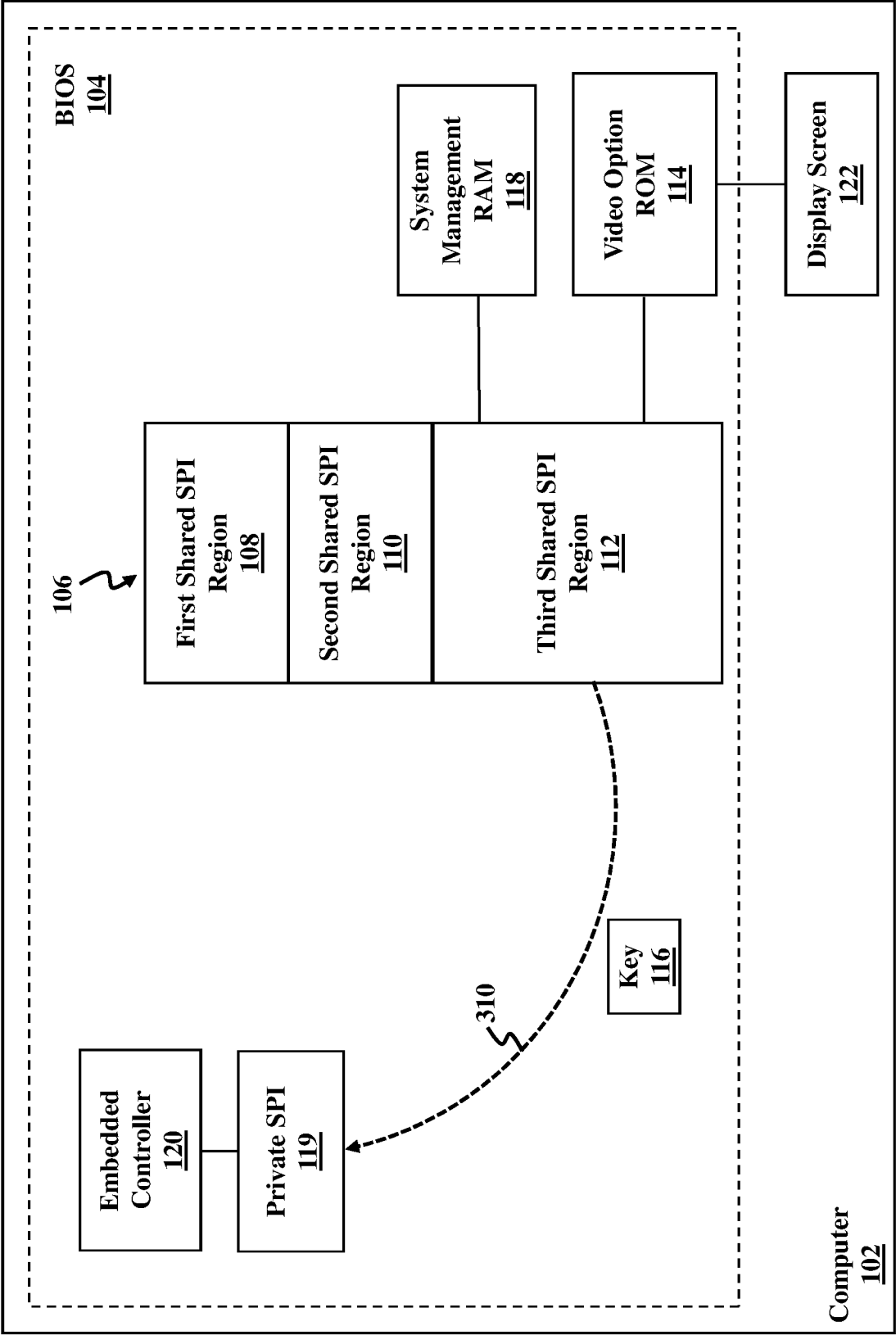


FIG. 3

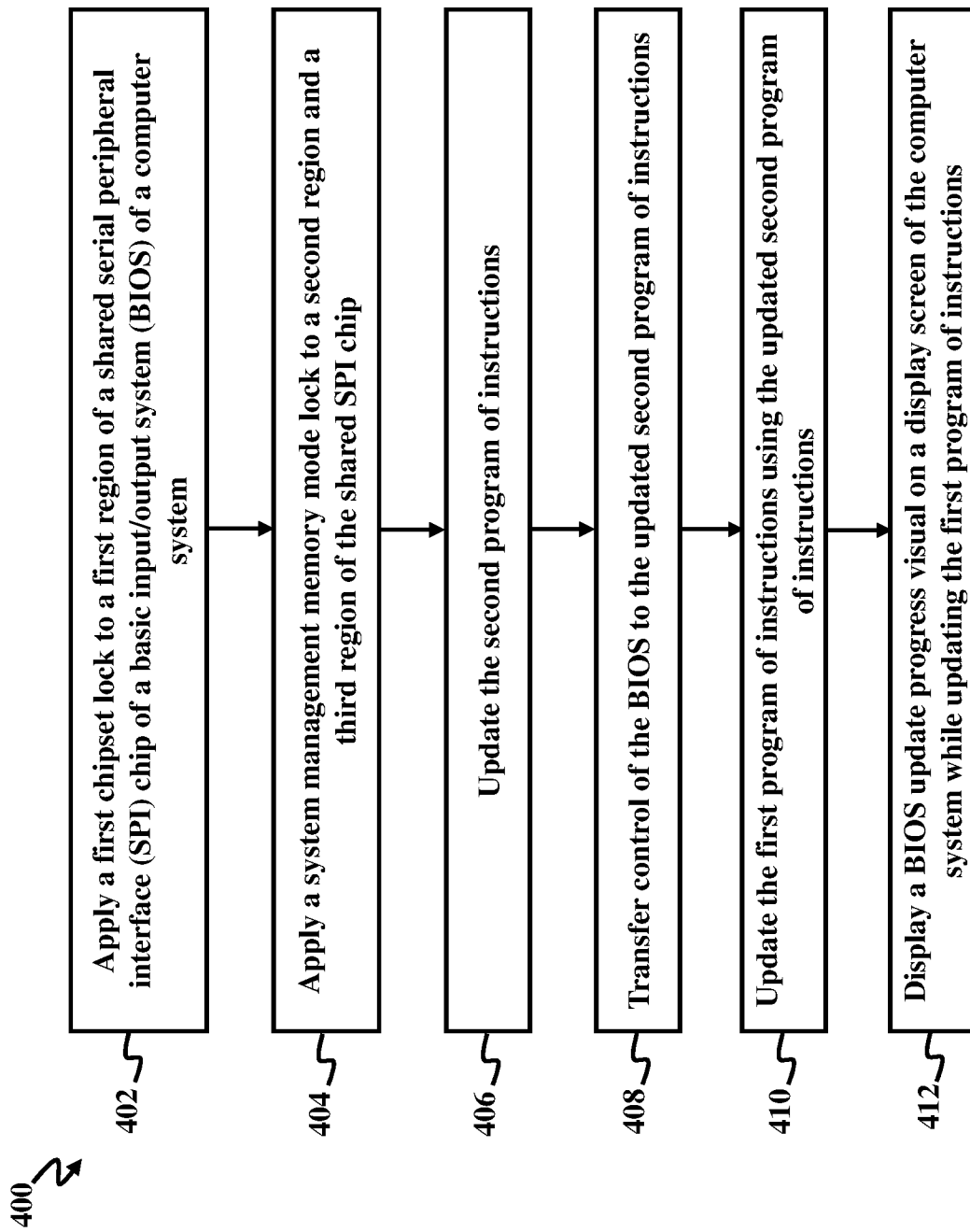


FIG. 4

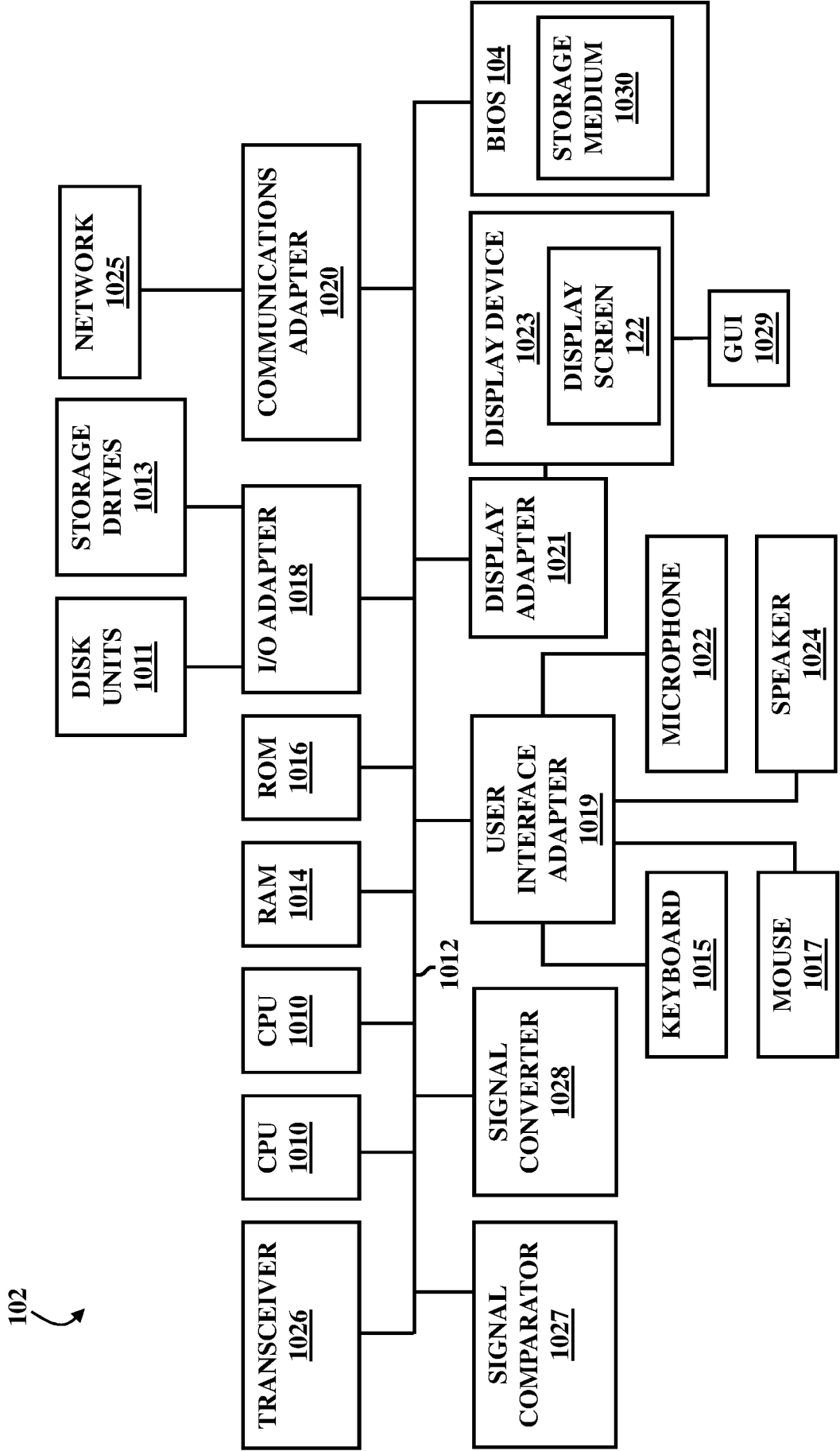


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2017/029129

A. CLASSIFICATION OF SUBJECT MATTER		
G06F 21/57 (2013.01) G06F 9/44 (2018.01)		
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 21/00-21/57, 9/00-9/44		
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 practicable, search terms used)		
PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Information Retrieval System of FIPS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/0147996 A1 (DELL PRODUCT, L.P.) 26.05.2016, paragraphs [0009], [0011], [0013], [0014], [0017], [0019], [0020]	1-15
A	US 2014/0040605 A1 (WILLIAM T. FUTRAL et al) 06.02.2014	1-15
A	US 7213152 B1 (ANDREW H.GAFKEN et al) 01.05.2007	1-15
A	US 6308265 B1 (GREGORY L.MILLER) 23.10.2001	1-15
☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.		
* Special categories of cited documents:	“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	
“A” document defining the general state of the art which is not considered to be of particular relevance	“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	
“E” earlier document but published on or after the international filing date	“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	
“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)	“&” document member of the same patent family	
“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		
Date of the actual completion of the international search	Date of mailing of the international search report	
30 January 2018 (30.01.2018)	07 February 2018 (07.02.2018)	
Name and mailing address of the ISA/RU: Federal Institute of Industrial Property, Berezhkovskaya nab., 30-1, Moscow, G-59, GSP-3, Russia, 125993 Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37	Authorized officer V. Volodin Telephone No. (499) 240-25-91	