(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2009 (29.01.2009)

PCT

(10) International Publication Number
WO 2009/014574 A1

(51) International Patent Classification:
H01R 13/639 (2006.01)

(21) International Application Number:
PCT/US2008/006575

(22) International Filing Date: 21 May 2008 (21.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/828,319 25 July 2007 (25.07.2007) US

(71) Applicant *(for all designated States except US)*: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 20555 S.H. 249, Houston, Texas 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NGUYEN, Vincent** [US/US]; 20555 Tomball Parkway, Houston, Texas 77070 (US). **HUA, Chanh V.** [US/US]; 20555 Tomball Parkway, Houston, Texas 77070 (US). **NGUYEN, Minh H.** [US/US]; 20555 Tomball Parkway, Houston, Texas 77070 (US). **NEUFELD, E. D.** [US/US]; 20555 Tomball Parkway, Houston, Texas 77070 (US).

(74) Agents: **WEBB, Steven L** et al.; Hewlett-Packard Company, Intellectual Property Administration, P.O. Box 272400, Mail Stop 35, Fort Collins, Colorado 80527-2400 (US).

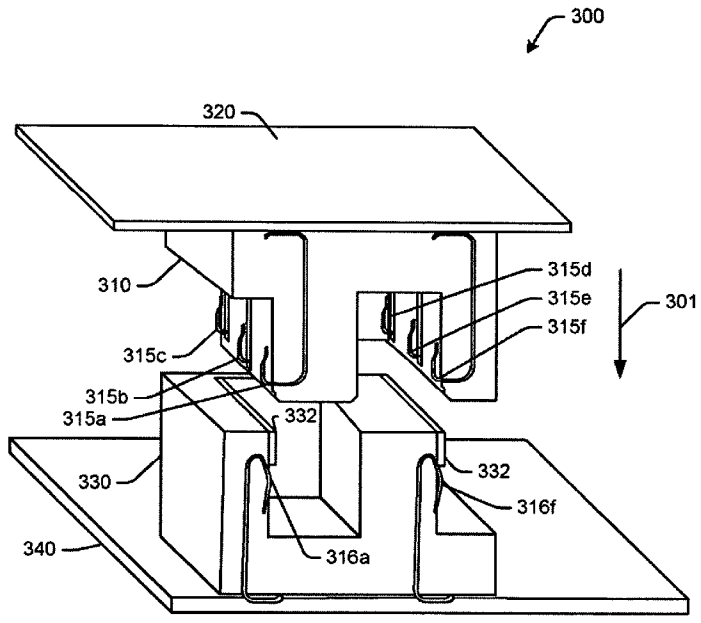
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: TAMPER-EVIDENT CONNECTOR

Fig. 3



(57) Abstract: Embodiments of a tamper-evident connector (200 or 300) are disclosed which may optionally be used in a trusted computing environment. In an exemplary embodiment, a tamper-evident connection includes a mate-once engaging assembly (310) for providing with a first component (320), the mate-once engaging assembly (310) including a foldable portion (315a). The tamper-evident connection also includes a receiving chamber (330) for providing with a second component (340), the mate-once engaging assembly (310) fitting in the receiving chamber (330) to physically secure the first component (320) to the second component (340), the foldable portion (315a) of the mate-once engaging assembly (310) unfolding during removal of the mate-once engaging assembly (310) from the receiving chamber (330) to provide evidence of tampering when the first component (310) has been removed from the second component (340). Optionally, the first component is a Trusted Platform Module (TPM) (165) and the second component is a system board (105).

WO 2009/014574 A1

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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

TAMPER-EVIDENT CONNECTOR

BACKGROUND

[0001] In an unsecured computer environment, a computer application may access any available computing resources with little or no consideration given to whether those resources are secure. There are many reasons, however, that it is desirable to control access to computing resources.

[0002] The Trusted Computing Group (TCG) was formed and has adopted an industry standard specification to enhance the security of computing environments. The goal is to deliver an enhanced hardware and operating system (OS) -based trusted computing platform (TCP) for customers to run their applications. With regard to hardware considerations, a Trusted Platform Module (TPM) has been introduced which includes a micro-controller that stores security information. The TPM is the root of trust to create a secured environment that enables the OS and applications to fight against software attacks. TCG requires the TPM identification to be unique and to physically bind to a specific platform such that it can not be

[0003]

[0004]

[0005] easily removed or transferred to another platform. Furthermore, the TPM must show evidence of physical tampering upon inspection.

[0006]

[0007]

[0008] Manufacturing platforms with the TPM increases the manufacturing costs. In addition, some countries (e.g., Russia and China) do not permit products to be shipped with security devices such as TPM. Accordingly, separate platforms without the TPM need to be manufactured and tracked (e.g., using unique SKU numbers) to be sold in these markets, thereby further increasing costs.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] **Figure 1** is a high-level illustration of an exemplary trusted computing platform (TCP).

[0010] **Figure 2** is a perspective view of an exemplary tamper-evident connector which may be implemented in a TCP.

[0011] **Figure 2a** is a perspective view of the exemplary tamper-evident connector in Figure 2 shown mounted to a system board in the TCP.

[0012] **Figure 2b** is a perspective view of the exemplary tamper-evident connector in Figure 2 after being removed from the system board.

[0013] **Figure 3** is a perspective view of another exemplary tamper-evident connector which may be implemented in a TCP.

[0014] **Figure 3a** is a perspective view of the exemplary tamper-evident connector in Figure 3 shown mounted to a system board in the TCP.

[0015] **Figure 3b** is a perspective view of the exemplary tamper-evident connector in Figure 3 after being removed from the system board.

DETAILED DESCRIPTION

[0016] Briefly, embodiments of a tamper-evident connector are disclosed. The designs enable the TPM to be manufactured separately as an optional component, thereby reducing the cost of manufacturing separate system boards for different markets, while still meeting the TCG physical binding requirement (i.e., there is visible evidence of tampering if the TPM is removed). After removal, a malformed TPM likely cannot be reused (or is difficult to reuse) in another system thereby maintaining the integrity of the trusted software environment (TSE) if the TPM has already been compromised. However, the removal process does not affect the system board, thereby allowing an authorized administrator to replace the TPM module on the system board if needed.

[0017] Although the systems and methods described herein help to enable security measures for running trusted software and accessing trusted resources, it is

[0018]

[0019] noted that application of the tamper-evident connector is not limited to computer security. Still other applications of the tamper-evident connector will be readily apparent to those having ordinary skill in the art after becoming familiar with the teachings herein.

[0020] **Figure 1** is a high-level illustration of an exemplary trusted computing platform (TCP) 100. Exemplary TCP 100 may include one or more processors or processing units 110, and a system memory 120, such as, e.g., read only memory (ROM) and random access memory (RAM) on system board 105. Other memory may also be provided (e.g., local and/or remote, fixed and/or removable, magnetic and/or optical media). The memory provides storage of computer-readable instructions, data structures, program modules and other data for computing platform 100.

[0021] It is noted that computing platform 100 may operate as a stand-alone device and/or may operate in a networked computing environment using logical connections to one or more remote resources (not shown). The logical connections may include a local area network (LAN) and/or a wide area network (WAN). Exemplary remote resources include, but are not limited to, a personal computer, a server, a router, a network PC, and a peer device or other network node. Remote resources may include many or all of the elements described for the computing platform 100, such as, e.g., processing capability and memory.

[0022]

[0023] Computing platform 100 may also include one or more resources 130a-c. As used herein, the term "resource" includes any of a wide variety of different types of devices (e.g., PCIe devices) and/or functions (e.g., provided by the device). In an exemplary embodiment, resources 130a-c may be communicatively

[0024] coupled to the computing platform 100 via one or more peripheral component interconnect (PCI) links 140a-b implementing the PCI-express (PCIe) specification. In such an embodiment, the resources 130a-c may be connected directly to the root complex 150 via one or more PCIe cards 145a-c.

[0025] A host bridge and memory controller hub, also referred to generally as a root complex 150, couples the various system components to the processing unit 110. The root complex 150 is a subsystem which detects and initializes resources 130a-c, and manages the links 140a-c so that processor 110 can read/write to the resources 130a-c and/or otherwise control the resources 130a-c.

[0026] Computing platform 100 may operate in a protected or trusted operating environment. A trusted operating environment is a protected or secured environment for running trusted software and accessing trusted devices. Trusted software is software that has a reliably established notion of identity, e.g., indicating that the software is from a trusted source. A trusted device is a device accessible via a Trusted Configuration Access Mechanism (TCAM) 160. It is noted

[0027]

[0028]

[0029] that there may be single or multiple TCAMs for each computing platform 100 (or for each partition on a computing platform).

[0030] The TCAM 160 is patterned after the Enhanced Configuration Access Mechanism (ECAM) provided for the standard configuration space defined by the PCIe specification (e.g., the ECAM 340 in Figure 3). Like the ECAM, the TCAM

[0031] 160 also includes memory mapped regions, 1 mega-byte (MB) per bus number, base addresses and bus number ranges reported by firmware. Unlike the ECAM, however, the TCAM 160 is usable only by the trusted software, optionally only when enabled by hardware, such as, e.g., a trusted platform module (TPM) 165. The TPM 165 provides protected storage, protected functions, authentication of the computing platform 100, measurement of platform integrity, and attestation of platform integrity. The TPM 165 may be implemented to assert a hardware signal that enables a TCAM 160 for use only if/when the platform integrity has been attested. The PCIe specification defines the TCAM, which then allows access to the trusted configuration registers via memory mapped address space, e.g., in memory 120.

[0032] The TPM 165 may be physically attached to the system board 105 by a tamper-evident connector. The tamper-evident connector provides visible evidence of tampering if the TPM 165 is removed from the system board 105 (e.g., in accordance with the TCG physical binding requirement). These and other features

[0033]

[0034] will be better understood by the description of exemplary embodiments of the tamper evident connector provided below with reference to Figures 2-3.

[0035] **Figure 2** is a perspective view of an exemplary tamper-evident connector which may be implemented in a TCP. In this embodiment, the tamper-

[0036] evident connector is implemented as a mechanical binding rivet 200. The mechanical binding rivet 200 (or simply "rivet 200") may include a pin 210 having a head portion 212 and a body portion 214. The rivet 200 may also include an outer housing member 220 having a chamber portion 222 and an expandable portion 224.

[0037] When the rivet 200 is used in a secure computing environment, an electrical connector 230 may be mounted adjacent the pin 210 on a first component (e.g., TPM 240), and a second electrical connector 235 may be mounted adjacent the housing member 220 on a second component (e.g., system board 250). In an exemplary embodiment, the first electrical connector 230 and second electrical connector 235 may be commercially available 20-pin (or any number pin) mating electrical connectors. In any event, the electrical connectors 230 and 235 can be pushed together to form an electrical connection between the TPM 240 and the system board 250, e.g., for transferring security information from the TPM 240 to the system board 250.

[0038] Before continuing, it is noted that although shown as separate parts, the pin 210 and housing member 220 may be manufactured as a single part having the functionality of both pin 210 and housing member 220. For example, the rivet 200 may be manufactured so that it can be shipped with the pin 210 loosely connected to the housing member 220 so that the parts are less likely to get misplaced or

[0039] otherwise lost. In addition, the electrical connectors 230 and 235 may also be integrated into the rivet 200 and do not need to be provided separately.

[0040] **Figure 2a** is a perspective view of the exemplary tamper-evident connector in Figure 2 shown mounted to a system board in the TCP. In use, the body portion 214 of the pin 210 may be slid through an opening formed in TPM 240 until the head portion 212 abuts the surface of TPM 240. The head portion 212 of the pin 210 serves to stop the pin from sliding entirely through the TPM 240.

[0041] The housing member 220 may be fit into an opening 252 formed in the system board 250. For example, slots 226 in the expandable portion 224 of the housing member 220 enable the housing member 220 to reduce in size (e.g., a smaller diameter) when it is squeezed to fit through the opening 252. A spring-action naturally returns the expandable portion 224 to a widened state within the opening 252 to at least partially hold the housing member 220 in the system board 250.

[0042] When the body portion 214 of the pin 210 slides into the expandable portion 224 of the housing member 220, the presence of pin 210 forces the expandable portion 224 of the housing member 210 to further widen within the opening 252. Optionally, the pin 210 may be wider (or may include "fins" or other devices) at the end to enhance forcing the expandable portion 224 open. This

[0043] widening action physically, and irreversibly, secures the TPM 240 to the system board 250.

[0044] **Figure 2b** is a perspective view of the exemplary tamper-evident connector in Figure 2 after being removed from the system board. Once connected, the electrical connection between electrical connectors 230 and 235 cannot be disconnected without removing the TPM 240 from the system board 250. However, in order for the TPM 240 to be removed from the system board 250, the expandable portion of the outer housing member must be broken apart to release the pin from the housing member, thereby providing visible evidence of tampering when the TPM 240 has been removed from the system board 250.

[0045] **Figure 3** is a perspective view of another exemplary tamper-evident connector which may be implemented in a TCP. In this embodiment, the tamper-evident connector is implemented as a "plug-type" connector 300. The plug-type connector (or simply "plug 300") may include a male block structure 310 for a first

[0046]

[0047]

[0048] component (e.g., TPM 320), and a female block structure 330 for a second component (e.g., system board 340).

[0049] The male block structure 310 includes at least one foldable pin (and a plurality of foldable pins 315a-c are shown in Figure 3), and the female block structure 330 includes a ledge portion 332. In an exemplary embodiment, the foldable pin(s) 315a-c are substantially hook-shaped or J-shaped, so that the

[0050] foldable pins contact the ledge portion 332 when the male block structure 310 is fit into the female block structure 330 to physically secure the TPM 310 to the system board 340.

[0051] **Figure 3a** is a perspective view of the exemplary tamper-evident connector in Figure 3 shown mounted to a system board in the TCP. When the plug 300 is used in a secure computing environment, the foldable pins 315a-c serve as an electrical connector, mating with pins 335 in the female block structure 330. Alternatively, separate electrical connections may be provided (e.g., integrated or adjacent the male and female block structures). When the male and female block structures 310 and 330 are connected to one another, an electrical connection is formed between the TPM 320 and the system board 340, e.g., for transferring security information from the TPM 320 to the system board 340.

[0052] **Figure 3b** is a perspective view of the exemplary tamper-evident connector in Figure 3. Once connected, the electrical connection cannot be

[0053]

[0054] disconnected without removing the TPM 320 from the system board 340. However, in order for the TPM 320 to be removed from the system board 340, the foldable pins 315a-c are pulled by the ledge portion 332 and unfold during as the male block structure 310 is pulled apart from the female block structure 330. This provides visible evidence of tampering when the TPM 320 has been removed from the system board 340.

[0055] It is noted that with regard to any of the embodiments of the tamper-evident connector described above, TPM installation (the initial binding process) may be performed by the system integrator during manufacturing by the original design manufacturer (ODM) or at customer sites. The use of tools is not necessary for the initial binding process, making the tamper-evident connector easy to use.

[0056] After removal, a malformed TPM likely cannot be reused (or is difficult to reuse) in another system thereby maintaining the integrity of the trusted software environment (TSE) if the TPM has already been compromised. However, the removal process does not affect the system board, thereby allowing an authorized administrator to replace the TPM module on the system board if needed, e.g., for servicing or replacement.

[0057] It is noted that the exemplary embodiments shown in the Figures and discussed above are provided for purposes of illustration. In addition to the specific embodiments explicitly set forth herein, other aspects and embodiments will be

[0058]

[0059] apparent to those skilled in the art from consideration of the specification disclosed herein. It is intended that the specification and illustrated embodiments be considered as examples only.

CLAIMS

1. A tamper-evident connector (300) comprising:

a mate-once engaging assembly (310) for providing with a first component (320), the mate-once engaging assembly (310) including a foldable portion (315a); and

a receiving chamber (330) for providing with a second component (340), the mate-once engaging assembly (310) fitting in the receiving chamber (330) to physically secure the first component (320) to the second component (340), the foldable portion (315a) of the mate-once engaging assembly (310) unfolding during removal of the mate-once engaging assembly (310) from the receiving chamber (330) to provide evidence of tampering when the first component (320) has been removed from the second component (340).

2. The tamper-evident connector (300) of claim 1 wherein the receiving chamber (330) is reusable with a different mate-once engaging assembly (310) after removal of the mate-once engaging assembly (310).

3. The tamper-evident connector (300) of claim 1 wherein the mate-once engaging assembly (310) is unusable with any receiving chamber (330) after

removal of the mate-once engaging assembly (310) from the receiving chamber (330).

4. The tamper-evident connector (300) of claim 1 wherein the mate-once engaging assembly (310) exhibits physical damage after removal of the mate-once engaging assembly (310) from the receiving chamber (330).

5. A tamper-evident connector (300) comprising:

a male block structure (310) for providing with a first component (320), the male block structure (310) including at least one foldable pin (315a);

a female block structure (330) for providing with a second component (340), the female block structure (330) including a ledge portion (332); and

wherein the male block structure (310) fits in the female block structure (330) to physically secure the first component (320) to the second component (340), the at least one foldable pin (315a) of the male block structure (310) contacting the ledge portion (332) of the female block structure (330) causing the foldable pin (315a) to unfold during removal of the male block structure (310) from the female block structure (330) to provide visible evidence of tampering when the first component (320) has been removed from the second component (340).

6. The tamper-evident connector (300) of claim 5 wherein the at least one foldable pin (315a) slides past the ledge portion (332) of the female block structure (330) during fitting of the male block structure (320) to the female block structure (330).

7. The tamper-evident connector (300) of claim 5 wherein the at least one foldable pin (315a) is embedded in the male block structure (310).

8. The tamper-evident connector (300) of claim 5 wherein the at least one foldable pin (315a) is electrically conductive and forms an electrical connection with at least one pin (316a) in the female block structure (330), and wherein the electrical connection provides a communications conduit between the first component (320) and the second component (340) for transferring security information.

9. A tamper-evident connector (200) comprising:

a pin having a head portion (210) and a body portion (214), the body portion (214) for sliding through a first component (240) until stopped by the head portion (210) abutting the first component (240);

an outer housing member (220) having a chamber portion (222) and an expandable portion (224) , the body portion (214) of the pin fitting into a second component (245); and

wherein the body portion (214) of the pin slides through the chamber portion (222) and into the expandable portion (224) of the outer housing member (220), the pin expanding the expandable portion (224) to physically secure the first component (240) to the second component (245), the expandable portion (224) of the outer housing member (220) breaking apart in order to release the pin from the outer housing member (220), thereby providing visible evidence of tampering when the first component (240) has been removed from the second component (245).

10. A tamper-evident connector (200 or 300) for use in secure computing environments, comprising:

a mate-once engaging assembly for a TPM (165); and

a receiving chamber for a system board (105), the mate-once engaging assembly fitting in the receiving chamber to physically secure the TPM (165) to the system board (105); and

a breakable portion providing visible evidence of tampering if the TPM (165) is removed from the system board (105).

Fig. 1

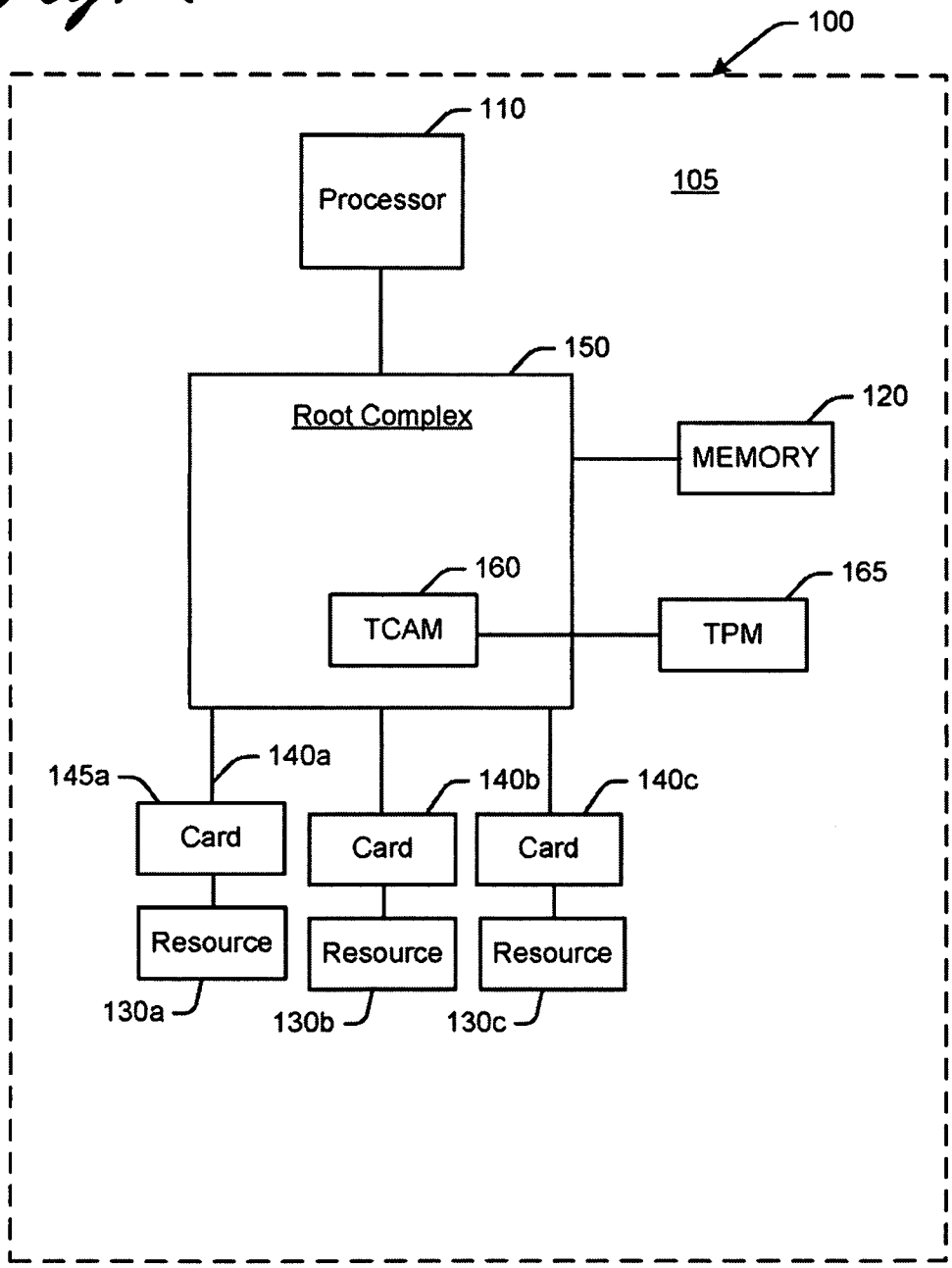

100
110
Processor
105
150
Root Complex
120
MEMORY
160
TCAM
165
TPM
145a
140a
140b
140c
Card
Card
Card
Resource
Resource
Resource
130a
130b
130c

Fig. 2

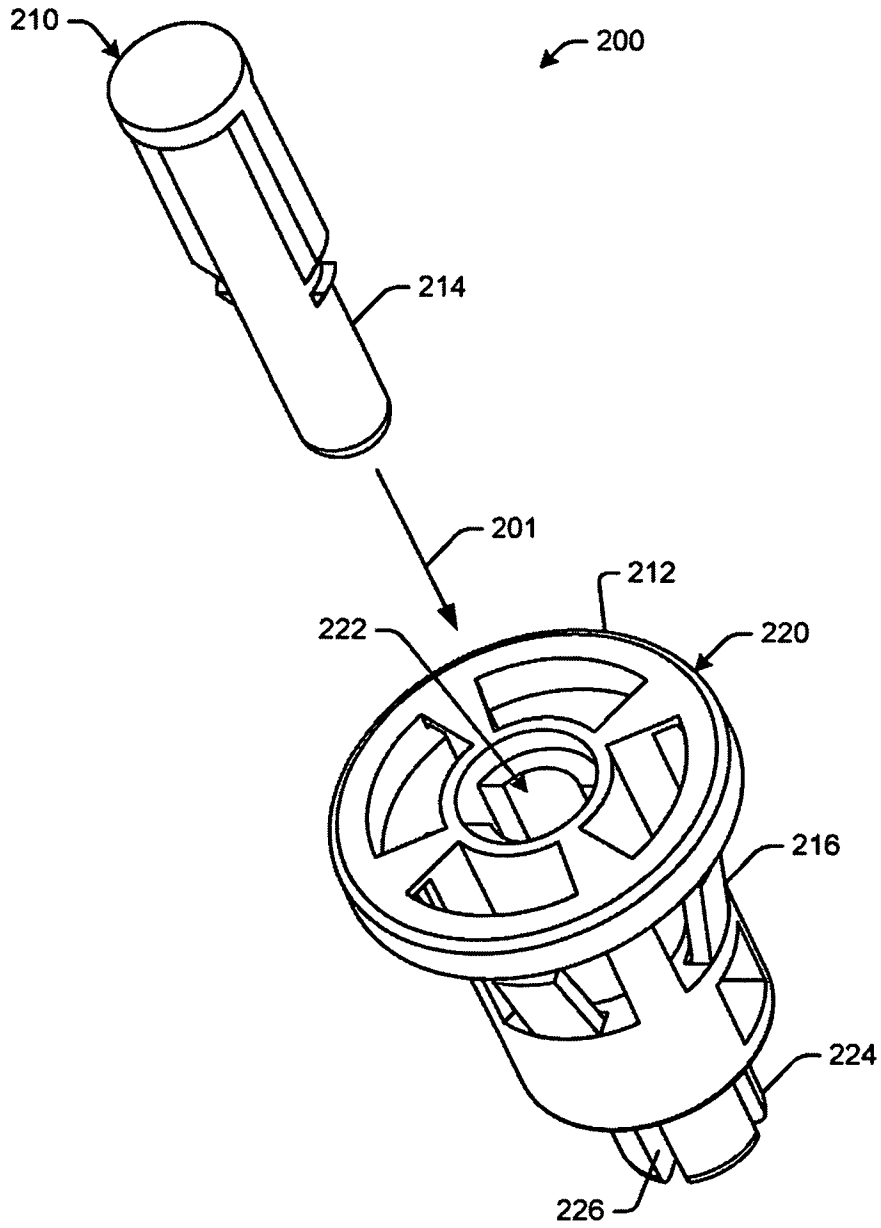


Fig. 2a

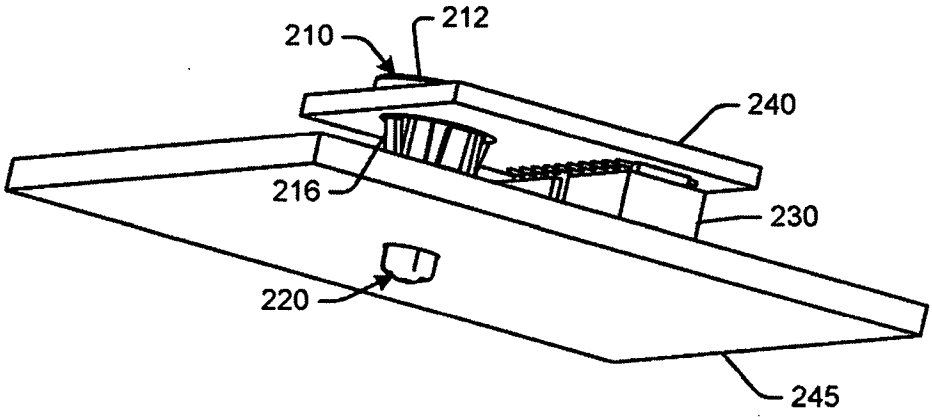


Fig. 2b

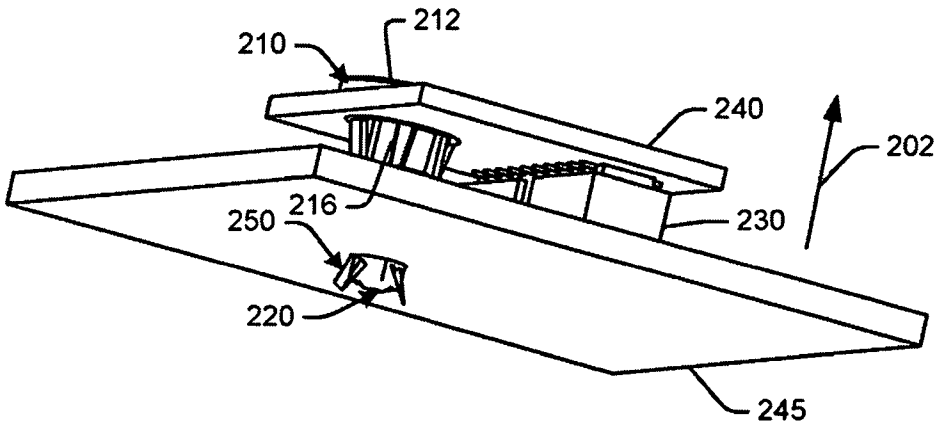


Fig. 3

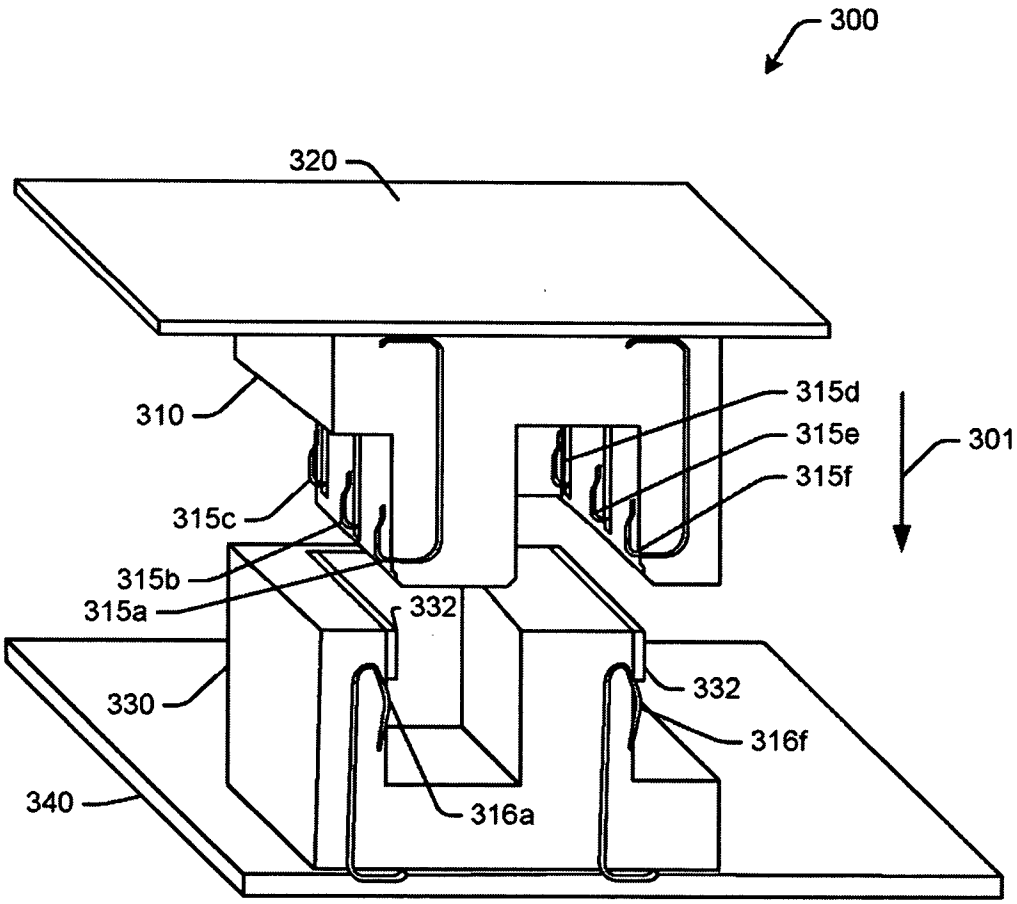

300
320
310
315d
315e
315f
301
315c
315b
315a
332
330
332
316f
340
316a

Fig. 3a

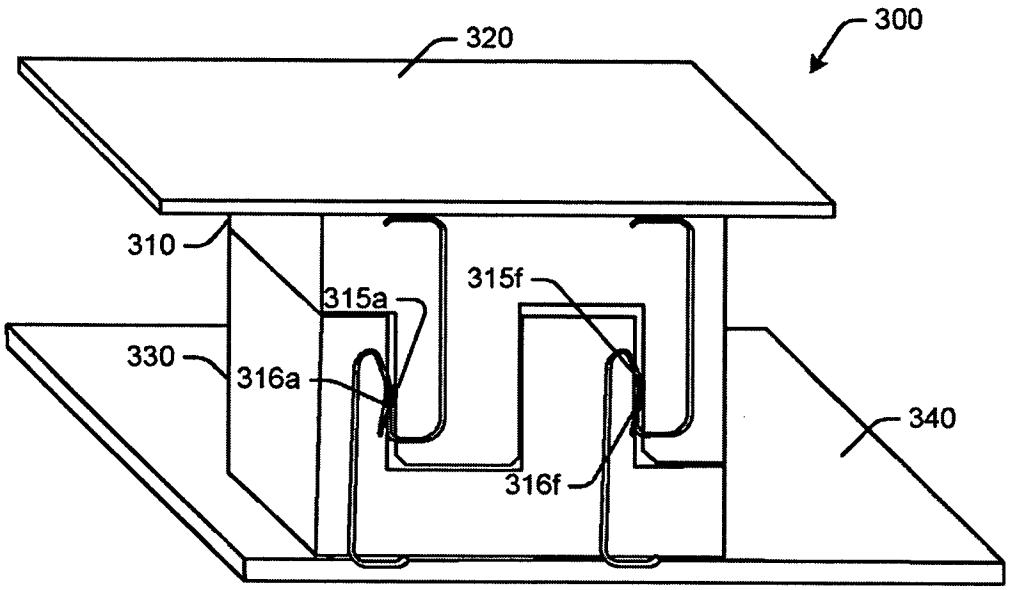
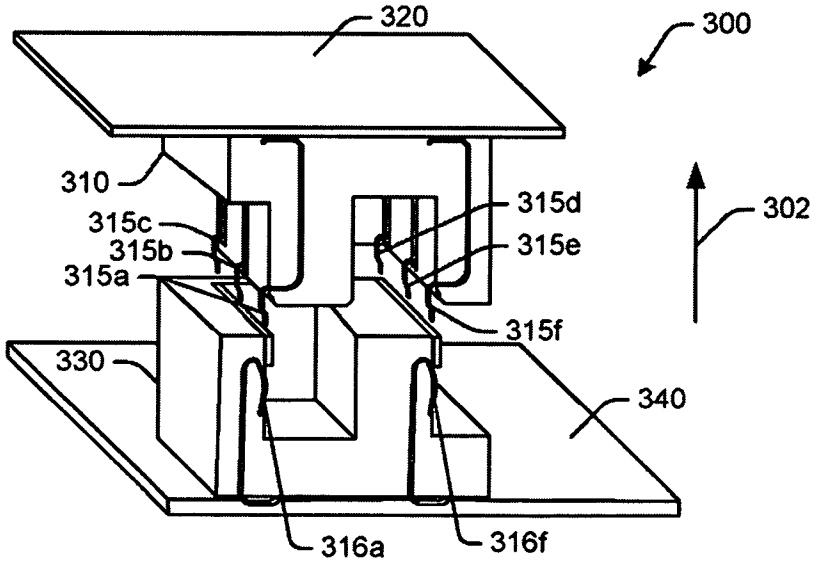

300
320
310
315a
315f
330
316a
340
316f

Fig. 3b


320
300
310
315c
315b
315a
315d
315e
315f
302
330
340
316a
316f

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/006575

A. CLASSIFICATION OF SUBJECT MATTER

H01R 13/639(2006.01)i

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)

IPC 8: H01R G08B

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

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

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

PAJ, FPD, USPAT, eKIPASS, IEEE "TAMPER" "EVIDENT/INDICATE/DETECT" "CONNECTOR"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7033193 B2 (Sidney A. Higgins) 25 APR 2006 see the abstract, figure 3, * column 3, line 33 - column 6, line 62 *	1-10
A	US 5785541 A (Gary R. Best) 28 JUL 1998 see the abstract, figure 1, * column 3, line 33 - column 5, line 38 *	1-10
A	US 4700384 A (Daniel Meyer) 13 OCT 1987 see the abstract, figure 2, * column 2, line 67 - column 5, line 47 *	1-10
A	US 7189109 B2 (Darrell Robinson) 13 MAR 2007 see the abstract, figure 3, * column 5, line 13 - column 11, line 67*	1-10
A	US 4990888 A (William R. Vogt, et al.) 05 FEB 1991 see the abstract, figure 5, * column 4, line 23 - column 8, line 39*	1-10

☐ 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 application or patent 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 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	Date of mailing of the international search report
30 OCTOBER 2008 (30.10.2008)	**31 OCTOBER 2008 (31.10.2008)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer NA, Sun Hee Telephone No. 82-42-481-5889

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/006575

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7033193 B2	25.04.2006	US 2005-266714 A1	01.12.2005
US 5785541 A	28.07.1998	NONE	
US 4700384 A	13.10.1987	NONE	
US 7189109 B2	13.03.2007	US 2005-122094 A1	09.06.2005
US 4990888 A	05.02.1991	CA 1268232 A1	24.04.1990