

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 August 2009 (06.08.2009)

PCT

(10) International Publication Number
WO 2009/096955 A1

(51) International Patent Classification:
G06F 12/16 (2006.01) **G06F 15/16** (2006.01)

(21) International Application Number:
PCT/US2008/052402

(22) International Filing Date: 30 January 2008 (30.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **HAINES, Matthew D.** [US/US]; 3404 E. Harmony Rd., Ft. Collins, 80528-9544 (US). **THERO, Daniel** [US/US]; 3404 E. Harmony Rd., Ft. Collins, 80528-9544 (US).

(74) Agent: **O'MEARA, William**; Hewlett-Packard Company, Intellectual Property Administration, Mail Stop 35, P.O. Box 272400, 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, 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))

Published:

- with international search report

(54) Title: ENCRYPTION BASED STORAGE LOCK

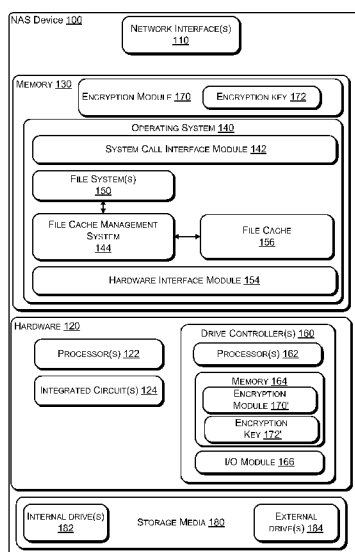


Fig. 1

(57) Abstract: In one embodiment an encryption based storage lock comprises at least one storage media, at least one processor, at least one drive controller, and logic to; store at least a first encryption key in a persistent memory location, establish a logical association between the first encryption key and a first drive, receive a write operation in a drive controller, wherein the write operation is associated with the first drive in the network attached storage device, encrypt data associated with the write operation using the first encryption key, and store the encrypted data in the first drive in the network attached storage device.

WO 2009/096955 A1

ENCRYPTION BASED STORAGE LOCK

BACKGROUND

[0001] The term Network Attached Storage (NAS) refers to a dedicated data storage device(s) connected directly to a computer network to provide centralized data access and storage services to one or more network clients such as, e.g., a personal computer. In some circumstances it may be useful to lock one or more storage media to a specific NAS device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Fig. 1 is a schematic illustration of an exemplary network attached storage device with an encryption lock.

[0003] Fig. 2A is a flowchart illustrating operations in one embodiment of an encryption lock in a network attached storage device.

[0004] Fig. 2B is a flowchart illustrating operations in one embodiment of an encryption lock in a network attached storage device.

[0005] Fig. 3 is a flowchart illustrating operations in one embodiment of an encryption lock in a network attached storage device.

[0006] Fig. 4 is a schematic illustration of a computing environment, according to some embodiments.

DETAILED DESCRIPTION

[0007] Described herein are exemplary systems and methods to implement an encryption-based storage lock in a network attached storage device. The methods described herein may be embodied as logic instructions stored on a computer-readable medium. When executed on a processor, the logic instructions cause a general processor to be programmed as a special-purpose machine that implements the described methods. The processor, when configured by the logic instructions to execute the methods recited herein, constitutes structure for performing the described methods.

[0008] **Fig. 1** is a schematic illustration of one embodiment of a network attached storage (NAS) device 100. Referring to Fig. 1, network storage device 100 comprises one or more network interfaces 110 which enable a communication connection with a network.

[0009] Network interface 110 may comprise an input/output (I/O) port to provide a physical connection with a network. For example, network interface 110 may comprise an Ethernet port. Network interface 110 may comprise a network interface card (NIC), also commonly referred to as a network adapter or a network card. The NIC manages I/O operations to enable NAS device 100 to communicate over a network. Alternatively, the operations of the NIC may be implemented on a main circuit board such as, e.g., a motherboard of NAS device 200.

[0010] NAS device further comprises hardware 120. The hardware 120 may comprise at least one integrated circuit 124 and in practice typically

comprises a plurality of integrated circuits 124. In some embodiments, the hardware 120 may comprise at least one processor 122. In some embodiments, a digital adapter may include a plurality of processors 122. As used herein, the term "processor" means any type of computational element, such as but not limited to, a microprocessor, a microcontroller, a complex instruction set computing (CISC) microprocessor, a reduced instruction set (RISC) microprocessor, a very long instruction word (VLIW) microprocessor, or any other type of processor or processing circuit.

[0011] In some embodiments, hardware 120 may comprise a drive controller 160. In some embodiments, a drive controller 160 may be a circuit which allows for communication with storage media such as a hard disk, floppy disk or the like. In some embodiments a drive controller 160 may comprise; one or more processors 162, memory 164, an encryption module 170' and encryption key 172' and an input/output module 166. In some embodiments, an input/output module 166 may comprise physical input output ports and logic that controls these input and output ports.

[0012] In operation, a drive controller 160 may receive, from a computing device on a network, input/output operations which write data to storage media 180 and transmit that data to one or more storage media 180. In addition, drive controller may receive input/output operations which read data from storage media 180. In some embodiments, a first encryption key 172' may be stored in a memory 164, and the encryption module 170' uses the encryption key to encrypt data written to and to decrypt data read from the storage media 180. In

addition, the encryption module 170' may further comprise logic to detect the removal of the drive controller 160 from the network attached storage device 100, and in response to the removal, disable the first encryption key 172'.

[0013] In some embodiments, encryption modules 170, 170' and encryption keys 172, 172' may be found in the NAS device hardware 120 and/or memory 130. In some embodiments, a NAS device may include an encryption module 170 in the NAS device which may generate an encryption key 172 for each drive and logically associate the encryption key 172 with the drive. In some embodiments, a drive vendor may generate an encryption key for each drive and store the encryption key in a predetermined memory location on the drive. In such embodiments, when a drive is plugged into the NAS device, the NAS device may retrieve the encryption key and stores it in a memory location such as ROM, and then may destroy the encryption key on the drive.

[0014] In some embodiments, a first encryption key may be stored in a read-only memory (ROM) module in the network attached storage device. The NAS device, alone or in combination with the ROM may implement a procedure in which at least a portion of the ROM is disabled when the ROM is removed from the NAS device. For example, NAS device 100 further comprises system random access memory and/or read-only memory, and the encryption key 172 is stored in a portion of the read-only memory. In one embodiment, if the NAS device ROM is removed from the NAS Device, a voltage sufficient to render inoperable the portion of the ROM in which the encryption key is stored is automatically applied thereby destroying the encryption key.

[0015] Memory 130 may comprise an operating system 140 for managing operations of NAS device 100. In one embodiment, operating system 140 comprises a hardware interface module 154 that provides an interface to system hardware. The particular embodiment of operating system 140 is not critical to the subject matter described herein. Operating system 140 may be embodied as a UNIX operating system or any derivative thereof (*e.g.*, Linux, Solaris, *etc.*) or as a Windows® brand operating system.

[0016] Operating system 140 comprises (or interfaces with) a file system(s) 150 that manages files used in the operation of NAS device 100. For example, file system(s) 150 may implement one or more of a Network File System (NFS) protocol, a Common Internet File System (CIFS) protocol, or the like. In one embodiment operating system 140 may comprise a file cache management system 144 interposed logically between the file system(s) 150 and underlying modules such as, *e.g.*, the hardware interface module 154. File cache management system 144 interfaces with the file system(s) 150 to manage the file cache 156 as a resource that may be shared between users of the computer system, *e.g.*, on a per-workload basis.

[0017] Operating system 140 further comprises a system call interface module 142 that provides an interface between the operating system 140 and one or more application modules that execute on NAS device 100.

[0018] NAS device 100 further comprises storage media 180. For example, storage media 180 may be embodied as one or more arrays of magnetic disk drives. Alternatively, storage media 180 may comprise optical,

magneto-optical, or electro-optical storage media. Storage media 180 may be configured to implement RAID redundancy. In some embodiments, storage media 180 may comprise at least one internal drive 182 or external drive 184. By way of example, and not limitation, an external drive 184 may comprise a flash memory drive, a diskette drive or the like.

[0019] NAS device 100 further comprises an encryption module 170. In some embodiments, an encryption module 170 is embodied in a NAS device memory 130. In some embodiments, an encryption module 170 is embodied in a NAS device hardware 120. In some embodiments, each encryption module 170 has a NAS device 100 specific encryption key 172. In operation, an encryption key 172 may lock data stored on attached storage media 180 to the specific NAS device 100. In some embodiments, an encryption module encrypts all data transmitted through a drive controller 160 with a NAS device specific encryption key 172. By way of example and not limitation, an encryption module 170 may use encryption protocols, such as, but not limited to, RSA encryption, or the like to encrypt data stored on a NAS device.

[0020] In some embodiments, a NAS device may contain an encryption key 172. By way of example and not limitation, an encryption key may use 128-bit, 256-bit or the like encryption. In some embodiments, a record of each NAS device encryption key 172 may be kept with an escrow service so as to allow a user to later retrieve the encryption key if needed. In operation, if a storage media is removed from a NAS device, access to the data on that storage media

is locked to the NAS device through the use of an encryption module 170 with a NAS specific encryption key 172.

[0021] In operation, if a storage media has been removed from a NAS device and anyone attempts to read any of the stored data, the data may be unreadable because the encryption key has locked the data to the specific NAS device. In operation, an encryption based drive lock may provide secure data protection while allowing for normal insertion and removal of drives within a specific NAS device.

[0022] **Fig. 2A** is a flowchart illustrating operations in one embodiment of an encryption lock in an network attached storage device. In some embodiments, the operations depicted in Fig. 2A are implemented by the encryption module 170 and/or 170'.

[0023] Referring to Fig. 2, at operation 205, a NAS device may store at least a first encryption key in a persistent memory location. In some embodiments, storing at least a first encryption key in a persistent memory location in a network attached storage device may comprise storing the encryption key in a read-only memory module in a drive controller in the network attached storage device. At operation 210, a NAS device may establish at least one logical association between a first encryption key and a first drive. At operation 215, a NAS device may receive a write operation for data on a first drive. By way of example and not limitation, the write operation may originate from over a network, from a direct link between a computing device and a NAS device or the like. In some embodiments, a computing device may initiate a

write operation without user input, such as but not limited to, when a computing device is performing a preprogrammed backup procedure or the like.

[0024] At operation 220, a NAS device may encrypt data using a first encryption key. By way of example and not limitation, an encryption key may use 128-bit, 256-bit or the like encryption.

[0025] At operation 225, a NAS device may store data on a first drive. In some embodiments, storage media may be internal or external drives. By way of example and not limitation, internal drives may include a hard disk drive, nonvolatile memory or the like. By way of example and not limitation, external drives may include thumb drives, handy drives, memory sticks, flash sticks, jump drives or the like.

[0026] In some embodiments, a NAS device may further comprise; storing at least a second encryption key in a persistent memory location in a network attached storage device, establishing a logical association between the second encryption key and a second drive in the network attached storage device, receiving a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the second drive in the network attached storage device, encrypting data associated with the write operation using the second encryption key, and storing, in a network attached storage device, the encrypted data in the second drive in the network attached storage device.

[0027] **Fig. 2B** is a flowchart illustrating operations in one embodiment of an encryption lock in a network attached storage device. In some

embodiments, the operations depicted in Fig. 2B are implemented by the encryption module 170 and/or 170'.

[0028] Referring to Fig. 2B, at operation 250 a first encryption key may be stored in a predetermined memory location associated with a first storage media. In some embodiments, a vendor may generate an encryption key for each drive and store the encryption key in a predetermined memory location on the drive. In such embodiments, when a drive is plugged into the NAS device, the NAS device may retrieve the encryption key and stores it in a memory location such as ROM, and then may destroy the encryption key on the drive.

[0029] At operation 255, a NAS device may couple a first storage media to a NAS device. In some embodiments, storage media may be internal or external drives. By way of example and not limitation, internal drives may include a hard disk drive, nonvolatile memory or the like. By way of example and not limitation, external drives may include thumb drives, handy drives, memory sticks, flash sticks, jump drives or the like.

[0030] At operation 260, a NAS device detects a first drive. In some embodiments, this detection process may occur during the boot phase of a NAS device.

[0031] At operation 265, a NAS device may retrieve a first encryption key from the first drive. At operation 270 a NAS device may store an encryption key in a ROM module. In some embodiments, a NAS device may store an encryption key in memory within a drive controller.

[0032] At operation 275 a NAS device may destroy a first encryption key on a first drive. In operation, destruction of the first drive encryption key may lock the first drive to the NAS device in that the data stored on the first drive may only be readable through the specific NAS device.

[0033] **Fig. 3** is a flowchart illustrating operations in one embodiment of a encryption lock in an network attached storage device. In some embodiments, the operations depicted in Fig. 3 are implemented by the encryption module 170 and/or 170'.

[0034] Referring to Fig. 3, at operation 310 a NAS device may receive a read operation for data on a first drive. In some embodiments, this read request may be made over a network, by a direct connection between a computing device and a NAs device or the like.

[0035] At operation 315, a NAS device may retrieve encrypted data from a first drive. At operation 320, a NAS device may decrypt data using a first encryption key. In some embodiments, an encryption key may be stored in a NAS device Rom memory. In some embodiments, an encryption key may be stored in a NAS device drive controller memory.

[0036] At operation 325, a NAS device returns the decrypted data. In some embodiments, the decrypted data may be transmitted over a network to a users computing device.

[0037] In some embodiments, an encryption-based hard drive lock may also be implemented in a computing environment. **Fig. 4** is a schematic

illustration of one embodiment of a computing environment. The components shown in Fig. 4 are only examples, and are not intended to suggest any limitation as to the scope of the functionality of the invention; the invention is not necessarily dependent on the features shown in Fig. 4.

[0038] Generally, various different general purpose or special purpose computing system configurations can be used. Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

[0039] The functionality of the computers is embodied in many cases by computer-executable instructions, such as program modules, that are executed by the computers. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Tasks might also be performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media.

[0040] The instructions and/or program modules are stored at different times in the various computer-readable media that are either part of the

computer or that can be read by the computer. Programs are typically distributed, for example, on floppy disks, CD-ROMs, DVD, or some form of communication media such as a modulated signal. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable media when such media contain instructions, programs, and/or modules for implementing the steps described below in conjunction with a microprocessor or other data processors. The invention also includes the computer itself when programmed according to the methods and techniques described below.

[0041] For purposes of illustration, programs and other executable program components such as the operating system are illustrated herein as discrete blocks, although it is recognized that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.

[0042] With reference to Fig. 4, the components of computer 400 may include, but are not limited to, a processing unit 404, a system memory 406, and a system bus 408 that couples various system components including the system memory 406 to the processing unit 404. The system bus 408 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard

Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as the Mezzanine bus, and PCI Express (PCIe).

[0043] Computer 400 typically includes a variety of computer-readable media. Computer-readable media can be any available media that can be accessed by computer 400 and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer-readable media may comprise computer storage media and communication media. "Computer storage media" includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by computer 400. Communication media typically embodies computer-readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media

includes wired media such as a wired network, fiber optic networks, or direct-wired connection and wireless media such as acoustic, RF, infrared and other wireless media. Combinations of any of the above should also be included within the scope of computer readable media.

[0044] The system memory 406 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 410 and random access memory (RAM) 412. A basic input/output system 414 (BIOS), containing the basic routines that help to transfer information between elements within computer 400, such as during start-up, is typically stored in ROM 410. RAM 412 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 404. By way of example, and not limitation, Fig. 4 illustrates operating system 416, application programs 418, other software components 420, and program data 422.

[0045] The computer 400 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, the computer system of Fig. 4 may include a hard disk drive 424 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 426 that reads from or writes to a removable, nonvolatile magnetic disk 428, and an optical disk drive 430 that reads from or writes to a removable, nonvolatile optical disk 432 such as a CD ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to,

magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 424 is typically connected to the system bus 408 through a non-removable memory interface such as data media interface 434, and magnetic disk drive 426 and optical disk drive 430 are typically connected to the system bus 408 by a removable memory interface.

[0046] The drives and their associated computer storage media discussed above and illustrated in Fig. 4 provide storage of computer-readable instructions, data structures, program modules, and other data for computer 400. In Fig. 4, for example, hard disk drive 424 is illustrated as storing operating system 416', application programs 418', software components 420', and program data 422'. Note that these components can either be the same as or different from operating system 416, application programs 418, software components 420, and program data 422. Operating system 416, application programs 418, other program modules 420, and program data 422 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 400 through input devices such as a keyboard 436 and pointing device 438, commonly referred to as a mouse, trackball, or touch pad. Other input devices (not shown) may include a microphone 440, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 404 through an input/output (I/O) interface 442 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel port, game port, or a universal serial bus (USB). A monitor 444 or other

type of display device is also connected to the system bus 406 via an interface, such as a video adapter 446. In addition to the monitor 444, computers may also include other peripheral output devices (*e.g.*, speakers) and one or more printers 470, which may be connected through the I/O interface 442.

[0047] The computer may operate in a networked environment using logical connections to one or more remote computers, such as a remote computing device 450. The remote computing device 450 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to computer 400. The logical connections depicted in Fig. 4 include a local area network (LAN) 452 and a wide area network (WAN) 454. Although the WAN 454 shown in Fig. 4 is the Internet, the WAN 454 may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the like.

[0048] When used in a LAN networking environment, the computer 400 is connected to the LAN 452 through a network interface or adapter 456. When used in a WAN networking environment, the computer 400 typically includes a modem 458 or other means for establishing communications over the Internet 454. The modem 458, which may be internal or external, may be connected to the system bus 406 via the I/O interface 442, or other appropriate mechanism. In a networked environment, program modules depicted relative to the computer 400, or portions thereof, may be stored in the remote computing device 450. By way of example, and not limitation, Fig. 4 illustrates remote application

programs 460 as residing on remote computing device 450. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0049] The terms "logic instructions" as referred to herein relates to expressions which may be understood by one or more machines for performing one or more logical operations. For example, logic instructions may comprise instructions which are interpretable by a processor compiler for executing one or more operations on one or more data objects. However, this is merely an example of machine-readable instructions and embodiments are not limited in this respect.

[0050] The terms "computer readable medium" as referred to herein relates to media capable of maintaining expressions which are perceivable by one or more machines. For example, a computer readable medium may comprise one or more storage devices for storing computer readable instructions or data. Such storage devices may comprise storage media such as, for example, optical, magnetic or semiconductor storage media. However, this is merely an example of a computer readable medium and embodiments are not limited in this respect.

[0051] The term "logic" as referred to herein relates to structure for performing one or more logical operations. For example, logic may comprise circuitry which provides one or more output signals based upon one or more input signals. Such circuitry may comprise a finite state machine which receives

a digital input and provides a digital output, or circuitry which provides one or more analog output signals in response to one or more analog input signals. Such circuitry may be provided in an application specific integrated circuit (ASIC) or field programmable gate array (FPGA). Also, logic may comprise machine-readable instructions stored in a memory in combination with processing circuitry to execute such machine-readable instructions. However, these are merely examples of structures which may provide logic and embodiments are not limited in this respect.

[0052] Some of the methods described herein may be embodied as logic instructions on a computer-readable medium. When executed on a processor, the logic instructions cause a processor to be programmed as a special-purpose machine that implements the described methods. The processor, when configured by the logic instructions to execute the methods described herein, constitutes structure for performing the described methods. Alternatively, the methods described herein may be reduced to logic on, e.g., a field programmable gate array (FPGA), an application specific integrated circuit (ASIC) or the like.

[0053] In the description and claims, the terms coupled and connected, along with their derivatives, may be used. In particular embodiments, connected may be used to indicate that two or more elements are in direct physical or electrical contact with each other. Coupled may mean that two or more elements are in direct physical or electrical contact. However, coupled

may also mean that two or more elements may not be in direct contact with each other, but yet may still cooperate or interact with each other.

[0054] Reference in the specification to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is comprised in at least an implementation. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment.

CLAIMS

What is claimed is:

1. A method, comprising:
 - storing at least a first encryption key in a persistent memory location in a network attached storage device;
 - establishing a logical association between the first encryption key and a first drive in the network attached storage device;
 - receiving a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the first drive in the network attached storage device;
 - encrypting data associated with the write operation using the first encryption key; and
 - storing, in a network attached storage device, the encrypted data in the first drive in the network attached storage device.
2. The method of claim 1, wherein storing at least a first encryption key in a persistent memory location in a network attached storage device comprises:
 - storing the first encryption key in a predetermined memory location associated with a first storage media;
 - coupling the first storage media to the network attached storage device
 - detecting, in the network attached storage device, the first storage media;
 - retrieving the first encryption key from the first storage media;
 - storing the encryption key in a read-only memory module in the network attached storage device; and
 - destroying the first encryption key on the first storage media.
3. The method of claim 1, wherein storing at least a first encryption key in a persistent memory location in a network attached storage device comprises storing the encryption key in a read-only memory module in a drive controller in the network attached storage device.

4. The method of claim 1, wherein encrypting data associated with the write operation using the first encryption key comprises:

retrieving the encryption key from the persistent memory location into an active memory location; and

processing, in a network attached storage device, data associated with the write operation through an encryption module.

5. The method of claim 1, further comprising:

receiving a read operation in a drive controller in the network attached storage device, wherein the read operation requests data with the first drive in the network attached storage device;

retrieving, from the first drive, data associated with the read operation;

decrypting the retrieved data associated with the read operation using the first encryption key; and

returning the data in response to the read operation.

6. The method of claim 1, further comprising:

storing at least a second encryption key in a persistent memory location in a network attached storage device;

establishing a logical association between the second encryption key and a second drive in the network attached storage device

receiving a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the second drive in the network attached storage device;

encrypting data associated with the write operation using the second encryption key; and

storing, in a network attached storage device, the encrypted data in the second drive in the network attached storage device.

7. The method of claim 1, wherein the first encryption key is stored in a read-only memory module in the network attached storage device, and further comprising:

detecting removal of the read-only memory module from the network attached storage device; and

in response to the removal, disabling the first encryption key on the read-only memory module.

8. The method of claim 1, wherein the first encryption key is stored in a memory module on a drive controller in the network attached storage device, and further comprising:

detecting removal of the drive controller from the network attached storage device; and

in response to the removal, disabling the first encryption key on the read-only memory module.

9. A network attached storage device comprising:
at least one storage media;
at least one processor;
at least one drive controller; and
logic to:
store at least a first encryption key in a persistent memory location in the network attached storage device;
establish a logical association between the first encryption key and a first drive in the network attached storage device
receive a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the first drive in the network attached storage device;
encrypt data associated with the write operation using the first encryption key; and
store, in the network attached storage device, the encrypted data in the first drive in the network attached storage device.
10. The network attached storage device of claim 9, further comprising logic to:
store the first encryption key in a predetermined memory location associated with a first storage media;
couple the first storage media to the network attached storage device
detect, in the network attached storage device, the first storage media;
retrieve the first encryption key from the first storage media;
store the encryption key in a read-only memory module in the network attached storage device; and
destroy the first encryption key on the first storage media.
11. The network attached storage device of claim 9, further comprising logic to store the encryption key in a read-only memory module in a drive controller in the network attached storage device.

12. The network attached storage device of claim 9, further comprising logic to:

retrieve the encryption key from the persistent memory location into an active memory location; and

process, in a network attached storage device, data associated with the write operation through an encryption module.

13. The network attached storage device of claim 9, further comprising logic to:

receive a read operation in a drive controller in the network attached storage device, wherein the read operation requests data with the first drive in the network attached storage device;

retrieve, from the first drive, data associated with the read operation;

decrypt the retrieved data associated with the read operation using the first encryption key; and

return the data in response to the read operation.

14. The network attached storage device of claim 9, further comprising logic to:

store at least a second encryption key in a persistent memory location in a network attached storage device;

establish a logical association between the second encryption key and a second drive in the network attached storage device

receive a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the second drive in the network attached storage device;

encrypt data associated with the write operation using the second encryption key; and

store, in a network attached storage device, the encrypted data in the second drive in the network attached storage device.

15. The network attached storage device of claim 9, further comprising logic to:

detect removal of the read-only memory module from the network attached storage device; and

in response to the removal, disable the first encryption key on the read-only memory module.

16. The network attached storage device of claim 9, further comprising logic to:

detect removal of the drive controller from the network attached storage device; and

in response to the removal, disable the first encryption key on the read-only memory module.

17. A computer program product comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

- store at least a first encryption key in a persistent memory location in a network attached storage device;

- establish a logical association between the first encryption key and a first drive in the network attached storage device;

- receive a write operation in a drive controller in the network attached storage device, wherein the write operation is associated with the first drive in the network attached storage device;

- encrypt data associated with the write operation using the first encryption key; and

- store, in a network attached storage device, the encrypted data in the first drive in the network attached storage device.

18. The computer program product of claim 17, further comprising logic instructions which, when executed on the processor, configures the processor to:

- store the first encryption key in a predetermined memory location associated with a first storage media;

- couple the first storage media to the network attached storage device

- detect, in the network attached storage device, the first storage media;

- retrieve the first encryption key from the first storage media;

- store the encryption key in a read-only memory module in the network attached storage device; and

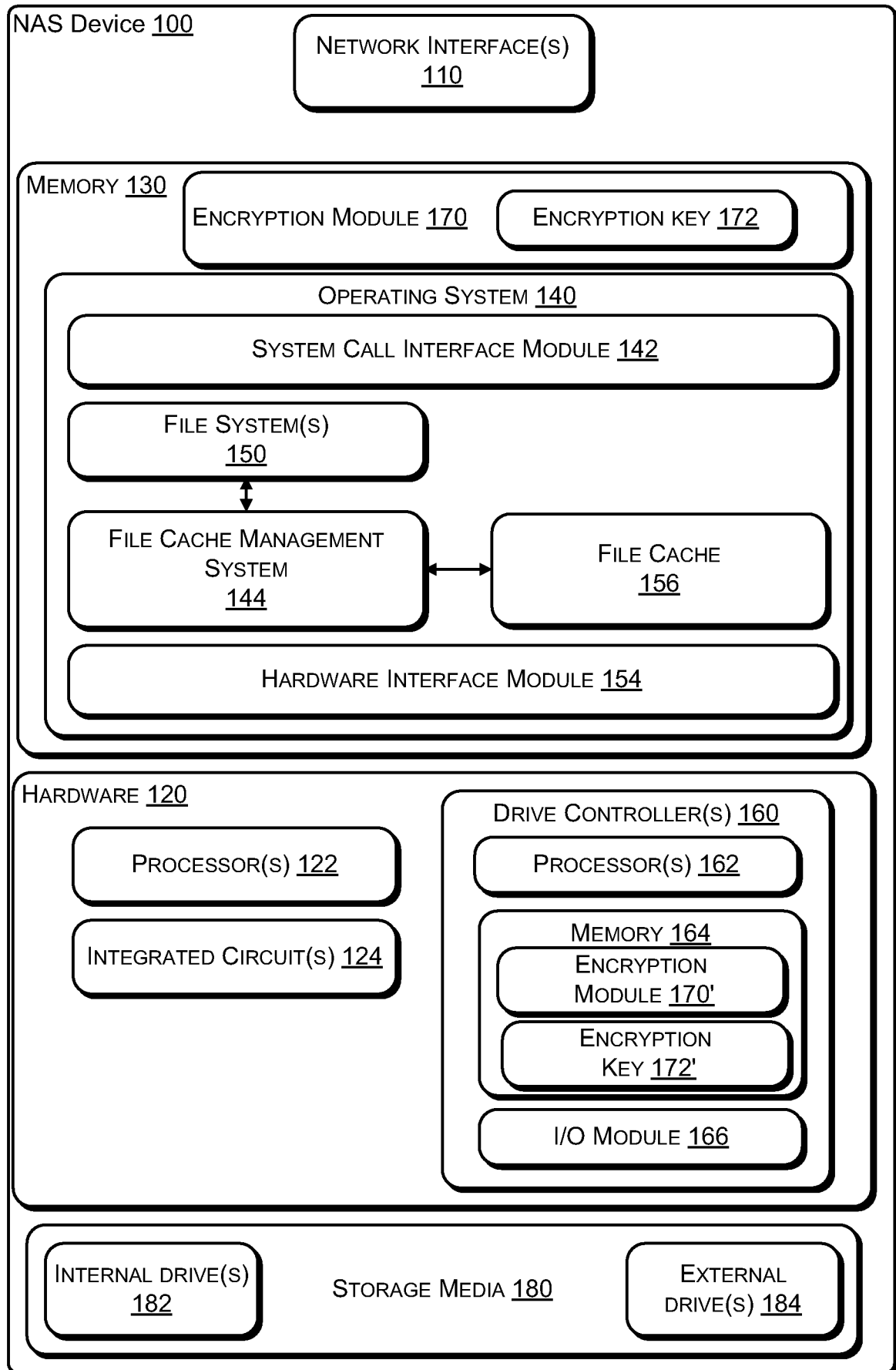
- destroy the first encryption key on the first storage media.

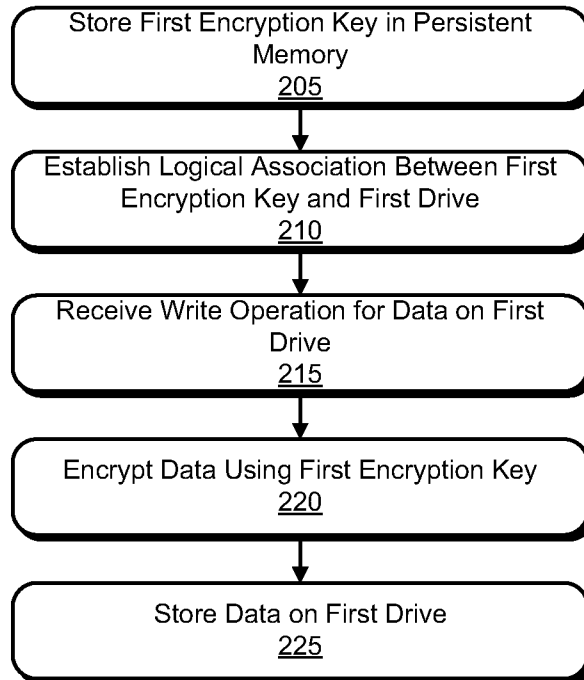
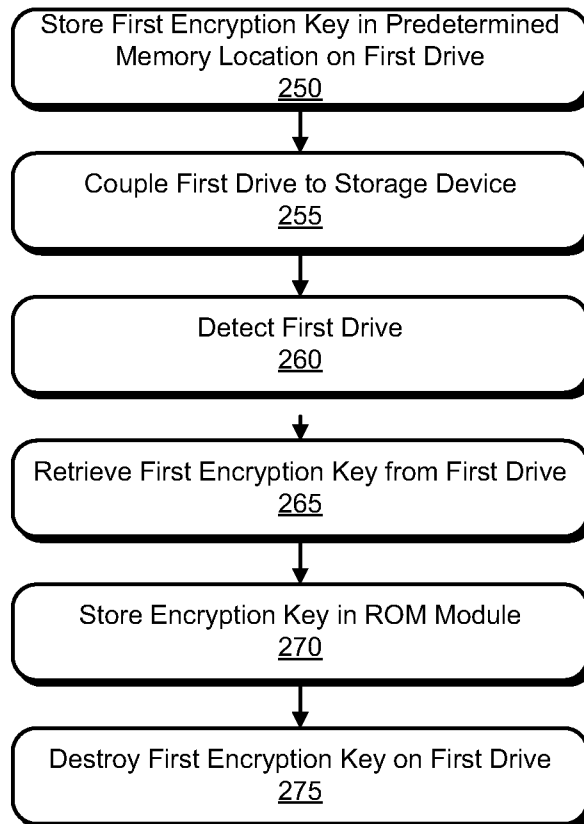
19. The computer program product of claim 17, further comprising logic instructions which, when executed on the processor, configures the processor to store the encryption key in a read-only memory module in a drive controller in the network attached storage device.

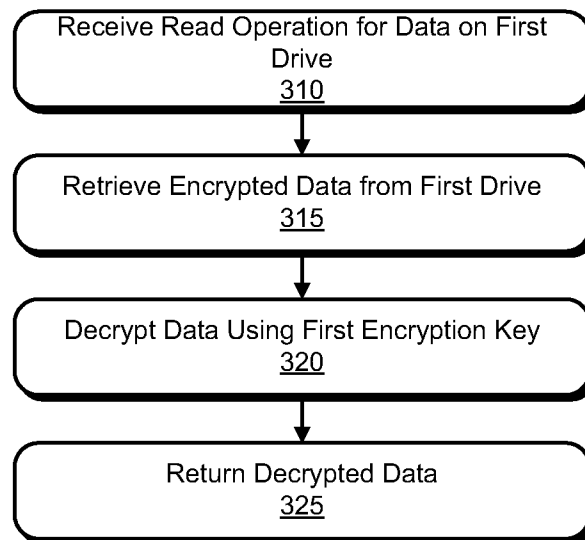
20. The computer program product of claim 17, further comprising logic instructions which, when executed on the processor, configures the processor to:

retrieve the encryption key from the persistent memory location into an active memory location; and

process, in a network attached storage device, data associated with the write operation through an encryption module.

**Fig. 1**

**Fig. 2****Fig. 2B**

**Fig. 3**

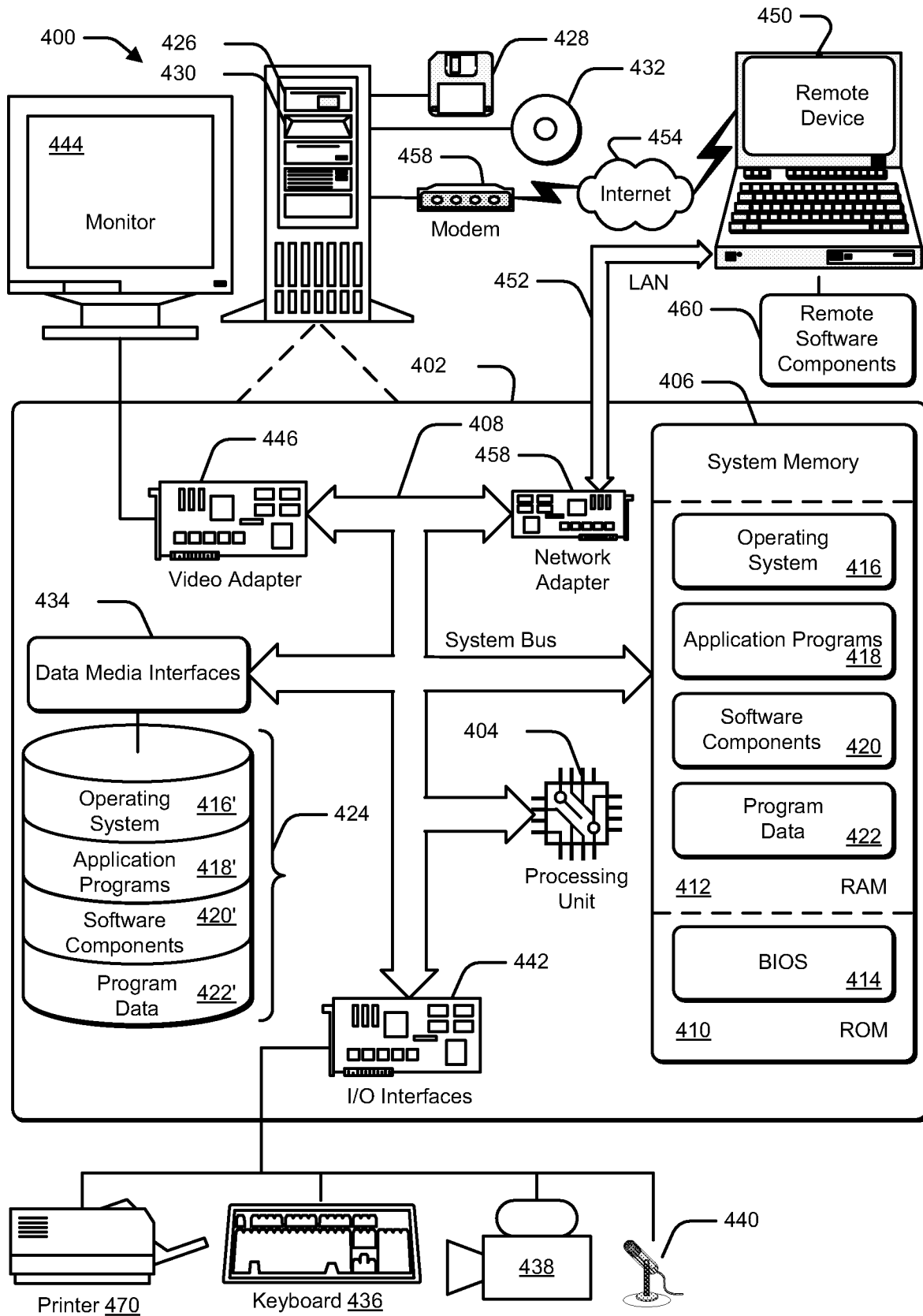


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/052402**A. CLASSIFICATION OF SUBJECT MATTER****G06F 12/16(2006.01)i, G06F 15/16(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 : G06F, H04L

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)

eKIPASS(KIPO internal) "encrypt", "network", "storage"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2006-0136735 A1 (PLOTKIN, S. et al.) 22 June 2006 See Abstract, Claims 1, 7, 15-21 and Figures 1-19.	1-6, 9-14, 17-20 7, 8, 15, 16
Y A	US 7,206,939 B2 (MIYAZAKI, K. et al.) 17 April 2007 See Abstract and Column 2, Line 14-Column 11, Line 25.	1-6, 9-14, 17-20 7, 8, 15, 16
Y A	WO 2006-124479 A2 (CISCO TECHNOLOGY, INC.) 23 November 2006 See Abstract and Page 15, Line 6-Page 27, Line 13.	1-6, 9-14, 17-20 7, 8, 15, 16
Y A	US 2005-0013441 A1 (KLEIN, Y.) 20 January 2005 See Abstract, Claims 1-9 and Figures 1-4.	1-6, 9-14, 17-20 7, 8, 15, 16

☐ 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

30 JANUARY 2009 (30.01.2009)

Date of mailing of the international search report

30 JANUARY 2009 (30.01.2009)

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

LEE, Sang Hun

Telephone No. 82-42-481-5914



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/052402

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0136735 A1	22.06.2006	AU 2002-305607 A8	25.11.2002
		EP 1388061 A2	11.02.2004
		US 2004-0153642 A1	05.08.2004
		WO 02-093314 A2	21.11.2002
		WO 02-093314 A3	15.05.2003
US 7,206,939 B2	17.04.2007	AU 2001-38879 A1	26.09.2002
		AU 2001-38879 B2	26.09.2002
		AU 3887901 A	26.09.2002
		AU 758676 B2	27.03.2003
		EP 1243999 A2	25.09.2002
		EP 1396958 A1	10.03.2004
		EP 1243999 A3	17.05.2006
		JP 2002-335241 A	22.11.2002
		JP 2004-104750 A	02.04.2004
		JP 2008-136247 A	12.06.2008
		SG 109449 A1	30.03.2005
		SG 120979 A1	26.04.2006
		US 2002-0023221 A1	21.02.2002
		US 2003-0187885 A1	02.10.2003
		US 2004-0123107 A1	24.06.2004
		US 2006-0059357 A1	16.03.2006
		US 7,134,021 B2	07.11.2006
		US 7,305,558 B1	04.12.2007
		US 7,44,1115 B2	21.10.2008
WO 2006-124479 A2	23.11.2006	EP 1880326 A2	23.01.2008
		US 7,475,142 B2	06.01.2009
		US 2005-0223014 A1	06.10.2005
		WO 2006-124479 A3	27.12.2007
US 2005-0013441 A1	20.01.2005	US 7,460,672 B2	02.12.2008