

(51) International Patent Classification:
G06F 3/06 (2006.01)(21) International Application Number:
PCT/JP2009/001483(22) International Filing Date:
31 March 2009 (31.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **HITACHI, LTD.** [JP/JP]; 6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 1008280 (JP).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MIWA, Kyoko** [JP/JP]; c/o Hitachi, Ltd. Systems Development Laboratory 1099 Ozenji, Asao-ku, Kawasaki-shi, Kanagawa, 2150013 (JP). **OSAKI, Nobuyuki** [JP/JP]; c/o Hitachi, Ltd. Systems Development Laboratory 1099 Ozenji, Asao-ku, Kawasaki-shi, Kanagawa, 2150013 (JP). **ASANO, Masayasu** [JP/JP]; c/o Hitachi, Ltd. Systems Development Laboratory 1099 Ozenji, Asao-ku, Kawasaki-shi, Kanagawa, 2150013 (JP).(74) Agent: **ISSHIKI & CO.**; Rookin-Shinbashi Bldg., 12-7, Shinbashi 2-chome, Minato-ku, Tokyo, 1050004 (JP).

(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, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

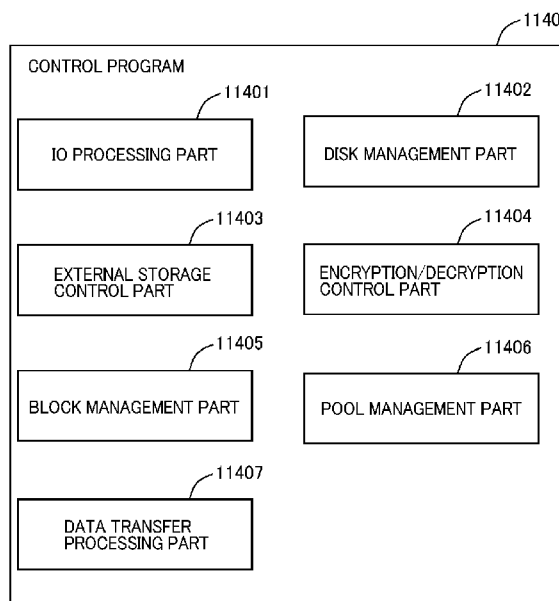
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, 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).

Published:

— with international search report (Art. 21(3))

(54) Title: STORAGE SYSTEM AND METHOD OF OPERATING THE SAME

[Fig. 4B]



(57) Abstract: A storage system comprising a storage apparatus having a storage control unit communicatively coupled to an external apparatus, forming a plurality of virtual storage areas each serving as a unit storage area used by the external apparatus as a data storing area, using a unit logical storage area selected among a plurality of unit logical storage areas provided by a physical storage medium, linking to each of the virtual storage areas, and any one of a plurality of attributes each representing a storage state of data stored in the virtual storage area, and maintaining the link wherein the storage control unit 11 further includes a logical storage area management unit 1140 that manages the link of the virtual storage area and any one of the attributes to each of logical storage area groups each configured to include the unit logical storage area to maintain the link and manage the linking relation, wherein the logical storage area management unit 1140, when receiving a command to change an attribute of any one of the virtual storage areas to a different attribute, determines presence or absence of the unit logical storage area that belongs to the logical storage area group linked to the changed different attribute and that is not yet allocated to any one of the virtual storage areas, and when determining the presence of the unit logical storage area that is not yet allocated to any one of the virtual storage areas,

the logical storage area management unit 1140 links the unit logical storage area determined to be present to the virtual storage area, reads out data stored in the unit logical storage area linked to a virtual storage area subjected to the attribute change, and stores the read data in the unit logical storage area determined to be present in accordance with a storage state represented by the different attribute.

Description

STORAGE SYSTEM AND METHOD OF OPERATING THE SAME

Technical Field

[0001] The present invention relates to a storage system and a method of operating the storage system, and, more particularly, to a storage system and a method of operating the storage system that simply and appropriately control an attribute representing a storing state of to-be-stored data for each virtual unit storage areas to simplify management configuration.

Background Art

[0002] A technique for dynamically extending a storage area provided to an external apparatus, such as a host computer, there is, for example, a so-called "thin provisioning" technique described in Patent Citation 1.

[0003] According to the thin provisioning technique described in Patent Citation 1, a host computer is provided with a virtual volume that is a virtual storage area by a storage apparatus communicatively coupled to the host computer. In addition, the storage apparatus has a pool area prepared thereto. The pool area is a group of logical devices that are logical storage areas (hereinafter "LDEV" or "logical volume"), and each LDEV is configured with a multiplicity of logical blocks (hereinafter "block") that are unit storage areas.

[0004] When receiving a data write request from the host computer, the storage apparatus allocates an unallocated block among blocks included in the pool area to a virtual volume.

[0005] The above storage apparatus may be configured so that a plurality of virtual volumes share the same pool area. In this case, each of the plurality of blocks belonging to the same pool area is allocated to a different virtual volume, respectively.

[0006] A need to keep data stored in the storage apparatus in an encrypted state may arise from the viewpoint of data security. For example, Patent Citation 2 discloses a storage apparatus that has a function of encrypting to-be-stored data to ensure the security of data stored in the storage apparatus.

Patent Citation 1: Japanese Patent Application Laid-Open Publication No. 2003-15915

Patent Citation 2: Japanese Patent Application Laid-Open Publication No. 2005-303981

Disclosure of Invention

Technical Problem

- [0007] In a storage apparatus having a configuration enabling thin provisioning for dynamically extending a storage area, a need may arise of specifying encrypting or not encrypting data to be stored in the storage apparatus not in units of virtual volumes but in units of physical storage areas, such as in units of parity groups. In this case, to encrypt all data written to a certain virtual volume, only the block belonging to a physical storage area that is given an instruction to be encrypted must be allocated to the virtual volume.
- [0008] To achieve this, a pool area as the source of block allocation is enabled to be specified for each virtual volume, and when data to be stored in a virtual volume is encrypted, a pool area configured with LDEVs including only the blocks to be encrypted (hereinafter "encryption LDEV") is specified for the virtual volume.
- [0009] A case is assumed, in which only the data stored in some of a plurality of virtual volumes is encrypted when the plurality of virtual volumes share a pool configured with LDEVs including only the blocks that are not to be encrypted (hereinafter "plain text LDEV"). To encrypt data stored in a virtual volume, a pool area configured with only the encryption LDEVs must be used. Therefore even in a case where a part of the virtual volumes are to be encrypted, all the LDEVs configuring the pool area shared by the virtual volumes must be encrypted. This poses a problem that even when a part of the virtual volumes are encrypted, the effect of encryption spreads to the other of the virtual volumes sharing the same pool area.
- [0010] A configuration so to manage an encrypted state in units of blocks to solve the above problem leads to a complicated management, thus ending up in an unrealistic solution. This problem applies to attributes in general that are to be set in units of physical storage areas with respect to data storing states including the above encrypted state.
- [0011] An object of the present invention is to provide a storage system and a method of operating the storage system that simply and appropriately control an attribute representing a storing state of to-be-stored data for each of virtual unit storage areas to simplify management configuration.

Technical Solution

- [0012] In order to solve the above and other problems, an aspect of the present invention provides a storage system comprising a storage apparatus having a storage control unit communicatively coupled to an external apparatus, forming a plurality of virtual storage areas each serving as a unit storage area used by the external apparatus as a data storing area, using a unit logical storage area selected among a plurality of unit logical storage areas provided by a physical storage medium, linking to each of the virtual storage areas, and any one of a plurality of attributes each representing a stored state of data stored in the virtual storage area, and maintaining the link wherein the

storage control unit further includes a logical storage area management unit that manages the link of the virtual storage area and any one of the attributes to each of logical storage area groups each configured to include the unit logical storage area to maintain the link and manage the linking relation, wherein the logical storage area management unit, when receiving a command to change an attribute of any one of the virtual storage areas to a different attribute, determines presence or absence of the unit logical storage area that belongs to the logical storage area group linked to the changed different attribute and that is not yet allocated to any one of the virtual storage areas, and when determining the presence of the unit logical storage area that is not yet allocated to any one of the virtual storage areas, the logical storage area management unit links the unit logical storage area determined to be present to the virtual storage area, reads out data stored in the unit logical storage area linked to a virtual storage area subjected to the attribute change, and stores the read data in the unit logical storage area determined to be present in accordance with a storage state represented by the different attribute.

Advantageous Effects

- [0013] According to the present invention there is provided a storage system and a method of operating the storage system that simply and appropriately control an attribute representing a storing state of to-be-stored data for each of virtual unit memory areas to simplify a management configuration.

Brief Description of the Drawings

- [0014] [fig.1]Fig. 1 is a diagram of a schematic configuration of storage system 1 according to one embodiment of the present invention.
- [fig.2]Fig. 2 is a diagram of an example of a hardware configuration of a computer that can be used as a management computer 20 and as a host computer 30.
- [fig.3]Fig. 3 is a diagram of an example of a software configuration of the host computer 30.
- [fig.4A]Fig. 4A is a diagram of an example of a configuration of a shared memory 114 of a storage apparatus 10.
- [fig.4B]Fig. 4B is a diagram of an example of a configuration of a control program 1140 stored in the shared memory 114.
- [fig.5]Fig. 5 is a diagram of an example of a software configuration of the management computer 20.
- [fig.6]Fig. 6 is a diagram of an example of a parity group management table 1141.
- [fig.7]Fig. 7 is a diagram of an example of an external volume group management table.
- [fig.8]Fig. 8 is a diagram of an example of an LDEV management table.

[fig.9]Fig. 9 is a diagram of an example of an external LDEV management table.

[fig.10]Fig. 10 is a diagram of an example of an LU management table.

[fig.11]Fig. 11 is a diagram of an example of a pool management table.

[fig.12]Fig. 12 is a diagram of an example of an allocated block management table.

[fig.13]Fig. 13 is a diagram of an example of an unallocated block management table.

[fig.14]Fig. 14 is a diagram of an example of a scheduled-to-be-deleted block management table.

[fig.15A]Fig. 15A is a diagram for explaining a general outline of a virtual volume encryption conversion process.

[fig.15B]Fig. 15B is a diagram for explaining a general outline of the virtual volume encryption conversion process.

[fig.15C]Fig. 15C is a diagram for explaining a general outline of the virtual volume encryption conversion process.

[fig.16]Fig. 16 is a diagram showing the relation between a physical storage area and a virtual storage area.

[fig.17]Fig. 17 is an example of a flowchart for explaining a process that is executed when the storage system according to one embodiment of the present invention receives an encryption instruction.

[fig.18A]Fig. 18A is an example of a flowchart for explaining an encrypted data transfer process that is executed by the storage system according to one embodiment of the present invention.

[fig.18B]Fig. 18B is an example of a flowchart for explaining the encrypted data transfer process that is executed by the storage system according to one embodiment of the present invention, showing a flowchart following the flowchart of Fig. 18A.

[fig.19A]Fig. 19A is a diagram of an example of a management screen that can be displayed on the management computer.

[fig.19B]Fig. 19B is a diagram of an example of a management screen that can be displayed on the management computer.

[fig.19C]Fig. 19C is a diagram of an example of a management screen that can be displayed on the management computer.

Embodiments of Invention

[0015] The present invention will now be described based on an embodiment thereof with reference to the accompanying drawings.

<Schematic Configuration of Storage System 1 of the Present Embodiment>

Fig. 1 is a diagram showing a schematic configuration of storage system 1 according to one embodiment of the present invention.

[0016] As shown in Fig. 1, the storage system 1 is configured to include one or more host computers (external apparatus) 30, one or more storage apparatuses 10, and an external

storage apparatus 40 that are coupled communicatively to each other via a storage network 51. The storage system 1 also includes a management computer 20 that is coupled communicatively to the storage apparatus 10 and to the external storage apparatus 40 via a management network 50. The external storage apparatus 40, which will be described later, is not a constituent element essential to the present invention.

[0017] The storage network 51 is a communication network that is used mainly for I/O-access-based communication between the host computer 30 and the storage apparatus 10. The storage network 51 is used also for I/O-access-based communication between the storage apparatus 10 and the external storage apparatus 40.

[0018] Such a network as SAN (Storage Area Network) and LAN (Local Area Network) can be adopted as the storage network 51, which is typically configured as a redundant system including a plurality of network switches, hubs, etc. In this embodiment, the storage network 51 is composed of a SAN (FC-SAN) based on the fiber channel (hereinafter "FC") protocol.

[0019] The management network 50 is a communication network that communicatively interconnects the management computer 20, the host computer 30, the storage apparatus 10, and the external storage apparatus 40. The management network 50 is used for communication that is carried when the management computer 20 manages the host computer 30, the storage apparatus 10, and the external storage apparatus 40. In this embodiment, the management network 50 is composed of a LAN based on the Internet protocol (hereinafter "IP").

[0020] (Host Computer 30)

The host computer 30 is a computer that executes, for example, an application program used for a business system in a bank, a seat reservation service system in an airline company, etc.

[0021] Fig. 2 depicts an example of a hardware configuration of a computer 1000 that can be used as the host computer 30 and as the management computer 20 to be described later. The computer 1000 has a central processing unit 1001 (e.g., CPU (Central Processing Unit), MPU (Micro Processing Unit), etc., which will hereinafter be referred to as "CPU" for simplicity), a main storage device 1002 (e.g., RAM (Random Access Memory), ROM (Read-Only Memory), etc.), an auxiliary storage device 1003 (e.g., hard disc drive (hereinafter "HDD")), an input device 1400 (e.g., keyboard, mouse, etc.) that receives user input, an output device 1005 (e.g., liquid crystal monitor), and a communication interface 1006 (e.g., NIC (Network Interface Card), HBA (Host Bus Adaptor), etc.) that realizes communication of the computer 1000 with another apparatus.

[0022] Fig. 3 depicts an example of a software configuration of the host computer 30. The host computer 30 has software resources including an operating system (hereinafter

"OS") 302 that provides a basic function as a computer, such as data I/O processing, and an application program 301 that runs on the OS 302. The host computer 30 thus executes the application program 301 varying in type under control by the CPU 1001 to realize desired processing through cooperation with other hardware resources.

[0023] Typically, in the process of executing an application program on an OS under control by the CPU, the host computer 30 accesses data stored in the storage apparatus 10 and the external storage apparatus 40, which will be described later, to realize desired business processing.

[0024] (Storage Apparatus 10)

The storage apparatus 10 is a subsystem that provides the host computer 30 with a storage area for storing data. As shown in Fig. 1, the storage apparatus 10 can be provided as, for example, an appropriate type of an RAID (Redundant Array of Independent (or Inexpensive) Disks) system including disk arrays having a plurality of HDDs (physical storage medium) 121. The HDD 121 may be replaced with another storage medium, such as a SSD (Solid State Drive).

[0025] The storage apparatus 10 includes a disk device 12, and a disk control unit 11 that executes data I/O processing between the host computer 30, data I/O processing between the HDD 121, and data I/O processing between the external storage apparatus 40.

[0026] The disk control unit 11 has a host interface (hereinafter "I/F") 111, a CPU 112, a cache memory (hereinafter "CM") 113, a shared memory (hereinafter "SM") 114, a disk IF 115, a management IF 116, and an external IF 117.

[0027] The host IF 111 is a communication interface that is provided for enabling communication between the host computer 30 and the storage apparatus 10. In this embodiment, the host IF 111 serves as a channel adaptor (hereinafter "CHA") coupled to the storage network 51 that is an FC network.

[0028] The CM 113 provides a storage area for temporarily storing therein data written to or read from the HDD 121.

[0029] The SM 114 has stored therein, for example, a program for controlling data I/O to/from the storage apparatus 10 and various management tables used for the control. The SM 114 has also stored therein a control program for executing a data encryption control process in this embodiment and management tables used by the control programs.

[0030] Figs. 4A and 4B depict an example of a configuration of the SM 114. The SM 114 has a control program 1140 functioning as a logical storage area management part, and management tables 1141 to 1149. The control program 1140 has various types of function parts for controlling the storage apparatus 10, the function parts including an I/O processing part 11401 that processes I/O access from the host computer 30, a disk

management part 11402 that controls I/O access to the disk device 12, an external storage control part 11403 that controls I/O access to the external storage apparatus, a encryption/decryption control part 11404 that encrypts and decrypts data to be stored in the HDD 121, a block management part 11405 that carries out block allocation and cancels block allocation to a virtual volume, a pool management part 11406 that manages a pool serving as a logical memory area group, and a data transfer processing part 11407 that encrypts plain text data already stored therein or decrypts encrypted data.

[0031] The block management part 11405 and the pool management part 11406 have a thin provisioning function of controlling block allocation to a virtual volume. The CPU 112 of the disk control unit 11 executes the control program 1140 to realize each of the above functions.

[0032] The SM 114 has stored therein a parity group management table 1141, an external volume group management table 1142, an LDEV management table 1143, an external LDEV management table 1144, an LU management table 1145, a pool management table 1146, an allocated block management table 1147, an unallocated block management table 1148, and a scheduled to-be-deleted block management table 1149. Details of the tables will be described later with reference to the drawings related to the tables.

[0033] The disk I/F 115 is a disk adaptor (hereinafter "DKA") serving as a communication interface that is provided to enable communication between the disk control unit 11 and the disk device 12.

[0034] The management I/F 116 is a communication interface that is provided to enable communication between the disk control unit 11 and the management computer 20. In this embodiment, the management I/F 116 is an NIC for connection to a LAN.

[0035] The external I/F 117 is a communication interface that is provided to enable communication between the storage apparatus 10 and the external storage apparatus 40. In this embodiment, the external I/F 117 is provided as a CHA coupled to the SAN, similar to the host I/F 111.

[0036] (External Storage Apparatus 40)

The external storage apparatus 40 has the same hardware configuration as that of the storage apparatus 10 that has been described above with reference to Fig. 1. The external storage apparatus 40 is capable of linking its logical volume to an external volume that is a virtual volume created in the external storage apparatus 40 by the storage apparatus 10. Through this linking, the logical volume of the external storage apparatus 40 is taken into the storage apparatus 10. And with an external connection technique, the logical volume taken in is regarded as a logical volume belonging to the storage apparatus 10. Thereby, the logical storage area is provided to the host computer

30 as storage resources incorporated in the storage apparatus 10.

[0037] (Management Computer 20)

The management computer 20 is a computer for managing the storage apparatus 10, and typically a general-purpose computer is used therefor. As described in Fig. 2, the management computer 20 has hardware resources including a CPU, a memory, a network I/F and the like.

[0038] Fig. 5 depicts an example of a software configuration of the management computer 20. The management computer 20 executes a management program 201 on an OS 202 under control by the CPU to provide a storage administrator with a user interface for managing the storage apparatus 10 and the external storage apparatus 40. In response to an input operation by the storage administrator, the management computer 20 carries out management of the storage system 1, such as giving instructions to execute setting and processing on the storage apparatus 10 and the external storage apparatus 40 and monitoring the operation status of the storage apparatus 10 and the external storage apparatus 40. For example, the management computer 20 carries out setting on an encrypted state of data stored in a virtual volume (validating/invalidating encryption), based on operation by the storage administrator.

[0039] More specifically, as described in a process flow of this embodiment to be described later, for example, the management computer 20 is capable of sending an encryption transfer process command for encrypting a virtual volume specified by the storage administrator to the storage apparatus 10 to encrypt data already stored in the storage apparatus 10 or in the external storage apparatus 40. The management computer 20 may not be provided as an independent computer as shown in Fig. 1, but may be incorporated in the storage apparatus 10 as a component introduced into the storage system 1, for example. The management computer 20 can have an appropriate hardware configuration other than the above hardware configuration.

[0040] Above is a description of a configuration example of the storage system 1 according to one embodiment of the present invention. This configuration is only exemplary, and the configuration of the storage system 1 of the present invention is not limited to the configuration that has been described above with the accompanying drawings.

[0041] <Management Table>

Configurations of various management tables used in a data encryption control method executed by the storage system 1 of the present embodiment will be described. Symbol "#" in each of the tables is a symbol representing number.

[0042] (Parity Group Management Table 1141)

Fig. 6 is a diagram showing a configuration example of the parity group management table 1141. The parity group management table 1141 is a table for managing the configuration of a parity group.

- [0043] As shown in Fig. 6, each of entries of the parity group management table 1141 includes a parity group number column 11411, a disk number column 11412, an RAID level column 11413, an encryption attribute column 11414, an encryption key column 11415, and an encryption method column 11416. "Parity group" is a group consisting of pieces of data that share the same parity data in a single RAID group.
- [0044] The parity group number column 11411 has recorded therein a parity group identification number that is an identification code given to each parity group provided by an RAID group of the storage apparatus 10. The disk number column 11412 has recorded therein a disk number that is an identification code given to each of HDDs 121 configuring each parity group. In the example of Fig. 6, parity group 1 is configured with disks 1 to 4.
- [0045] The RAID level column 11413 has recorded therein the RAID level of an RAID group configuring each parity group. In the example of Fig. 6, each parity group is configured with a RAID level of 5.
- [0046] The encryption attribute column 11414 has recorded therein an encryption attribute representing performing or not performing encryption of data to be stored in each parity group. Specifically, when an encryption attribute is a "plain text", data remaining in the form of a plain text is stored in the parity group. When an encryption attribute is "cipher", data is encrypted to store the encrypted data in the parity group.
- [0047] When "cipher" is recorded in the encryption attribute column 11414, the encryption key column 11415 and the encryption method space 11416 has recorded therein an encryption key and an encryption method that are used for encrypting data to be stored in the parity group, respectively. The example of Fig. 6 indicates that data encryption is set for a parity group 2, and that data is encrypted by a encryption method "AES-CBC-256" (AES-CBC method encryption algorithm with key length of 256 bits) recorded in the encryption method column 11416, using a key "0x12345678" recorded in the encryption key column 11415. An encryption algorithm, an encryption mode, key length, etc., as an encryption method are not limited to the example of Fig. 6, but may be determined in an appropriate manner.
- [0048] (External Volume Group Management Table 1142)
- Fig. 7 is a diagram showing a configuration example of the external volume group management table 1142. The external volume group management table 1142 is a table for managing the configuration of an external volume group, which is a storage area provided by one or more HDDs 121 incorporated in the external storage apparatus 40. Specifically, the external volume group is formed to include a logical volume provided by the external storage apparatus 40.
- [0049] As shown in Fig. 7, each of entries of the external volume group management table 1142 includes an external volume group number column 11421, a WWN column

11422, a LUN column 11423, an encryption attribute column 11424, an encryption key column 11425, and an encryption method column 11426.

[0050] The external volume group number column 11421 has recorded therein an external volume group number that is an identification code for identifying each external volume group. The WWN column 11422 has recorded therein a WWN that is allocated to the CHA coupled to a logical volume of the external storage apparatus 40 that is linked to each external volume group.

[0051] The LUN column 11423 has recorded therein LUN that is given to a logical volume of the external storage apparatus 40 that corresponds to each external volume group. The encryption attribute column 11424, the encryption key column 11425, and the encryption method column 11426 has recorded therein information on encryption of each external volume group, and correspond to the same columns in the parity group management table 1141.

[0052] (LDEV Management Table 1143)

Fig. 8 depicts a configuration example of the LDEV management table 1143. The LDEV management table 1143 is a table for managing the configuration of an LDEV that is a logical volume created on a parity group. As shown in Fig. 8, each of entries of the LDEV management table 1143 includes a parity group number column 11431, an LDEV number column 11432, a start address column 11433, and an end address column 11434.

[0053] The parity group number column 11431 is identical with the same parity group number column on the parity group management table 1141 of Fig. 6. The LDEV number space 11432 has recorded therein an LDEV number that is an identification code for identifying each of LDEVs created on each parity group. The start address column 11433 and the end address column 11434 have recorded therein the LBA of the start block and the same of the end block of a plurality of blocks configuring the corresponding LDEV, respectively. The example of Fig. 8 indicates that each LDEV includes 200 blocks.

[0054] (External LDEV Management Table 1144)

Fig. 9 depicts a configuration example of the external LDEV management table 1144. The external LDEV management table 1144 is a table for managing the configuration of an LDEV that is a logical volume created on an external volume group. As shown in Fig. 9, each of entries of the external LDEV management table 1144 includes an external volume group number column 11441, an LDEV number column 11442, a start address column 11443, and an end address column 11444. Items recorded in the above columns are identical with items recorded in the corresponding columns on the LDEV management table 1143 of Fig. 8.

[0055] As described above, an LDEV provided by the external storage apparatus 40 is

coupled externally to the disk control unit 11 of the storage apparatus 10, and is used as a data storage area for the host computer 30 in the same manner as an LDEV provided by the HDD 121 in the storage apparatus 10.

[0056] (LU Management Table 1145)

Fig. 10 depicts a configuration example of the LU management table 1145. The LU management table 1145 is a table for managing the configuration of each LU that is a virtual volume provided to the host computer 30. As shown in Fig. 10, each of entries of the LU management table 1145 includes a virtual volume number column 11451, a WWN column 11452, an LUN column 11453, a capacity column 11454, and a pool number column 11455. This table indicates the corresponding relation between a virtual volume recognized by the host computer 30 as a data storage area and an LDEV actually constituting the virtual volume.

[0057] The virtual volume number column 11451 has recorded therein a virtual volume number that is an identification code for identifying each virtual volume provided to the host computer 30. The WWN column 11452 has recorded therein a WWN that is allocated to the CHA used by each virtual volume for data I/O to/from the host computer 30.

[0058] The LUN space 11453 has recorded therein an LUN given to each virtual volume. The capacity column 11454 has recorded therein a storage capacity allocated to each virtual volume. The pool number column 11455 has recorded therein a pool number that is an identification code for identifying a pool to which a block making up each virtual volume belongs.

[0059] (Pool Management Table 1146)

Fig. 11 depicts a configuration example of the pool management table 1146. The pool management table 1146 is a table for managing the configuration of each pool. As shown in Fig. 11, each of entries of the pool management table 1146 includes a pool number column 11461, an LDEV number column 11462, a pool capacity column 11463, a pool use ratio column 11464, an encryption attribute column 11465, and an encryption method column 11466.

[0060] The pool number column 11461 has recorded therein a pool number that is an identification code given to each pool to distinguish one pool from another. The LDEV number column 11462 has recorded therein an LDEV number that is an identification code given to each of LDEVs making up each pool. The pool capacity column 11463 has recorded therein the size of a storage area that each pool has. The pool use ratio column 11464 contains a record of a ratio of a capacity used for data storage to the memory capacity of each pool. Based on the value of a use ratio recorded in the pool use ratio space 11464, whether a block belonging to the pool can be allocated to a virtual volume is determined. A free capacity remaining in the pool, instead of a pool

use ratio, may actually be recorded in the pool use ratio column 11464.

- [0061] The encryption attribute column 11465 has recorded therein an encryption attribute of an LDEV that can be registered with each pool. This means that only the LDEV formed on a parity group whose encryption attribute is "cipher" can be registered with a pool whose encryption attribute is recorded as "cipher". In contrast, only the LDEV formed on a parity group whose encryption attribute is "plain text" can be registered with a pool whose encryption attribute is recorded as "plain text".
- [0062] The encryption method space 11466 has recorded therein data on an encryption method (corresponding to the same item on the parity group management table 1141 of Fig. 6) only when an encryption attribute of the pool is "cipher". This means that, for example, only the LDEV storing therein data encrypted by an encryption method identical with an encryption method recorded in the encryption method column 11466 can be registered with the pool. If "cipher" is recorded in the encryption attribute column 11465 but an encryption method is not recorded in the encryption method column 11466, registering an LDEV encrypted by an arbitrary encryption method may be allowed.
- [0063] (Allocated Block Management Table 1147)
 Fig. 12 depicts a configuration example of the allocated block management table 1147. The allocated block management table 1147 is a table for managing the configuration of a block allocated to each LU that is a virtual volume. As shown in Fig. 12, each entry of the allocated block management table 1147 includes an LUN column 11471, a start address column 11472, an end address column 11473, an LDEV number column 11474, a start address column 11475, and an end address column 11476.
- [0064] The LUN column 11471 has recorded therein an LUN that is an identification code given to each LU. The start address column 11472 and the end address column 11473 has recorded therein an LBA representing the start block and that of an LBA representing the end block of each logical address range configuring each LU, respectively. The LDEV number column 11474 has recorded therein an LDEV number given to an LDEV including a block allocated to each LU. The start address column 11475 and the end address column 11476 contain a record of the LBA of the start block and that of the end block of blocks each allocated to each UL.
- [0065] (Unallocated Block Management Table 1148)
 Fig. 13 depicts a configuration example of the unallocated block management table 1148. The unallocated block management table 1148 is a table for managing the configuration of a block that is not allocated yet to an LU, i.e., a block that can be newly allocated to an LU. As shown in Fig. 13, each of entries of the unallocated block management table 1148 includes a pool number column 11481, an LDEV number column 11482, a start address column 11483, and an end address column 11484.

[0066] The pool number column 11481 has recorded therein the pool number of a pool having an unallocated LDEV, and the LDEV number column 11482 has recorded therein the LDEV number of an LDEV including an unallocated block. The start address column 11483 and the end address column 11484 has recorded therein the LBA of the start block and that of the end block of blocks not allocated yet to an LU among blocks making up each LDEV registered with a pool.

[0067] (Scheduled-to-Be-Deleted Block Management Table 1149)

Fig. 14 depicts a configuration example of the scheduled-to-be-deleted block management table 1149. The scheduled-to-be-deleted block management table 1149 is a table for managing the configuration of a scheduled-to-be-deleted block that is a block already released from allocation to an LU to maintain storage data to be deleted. As shown in Fig. 14, each of entries of the scheduled-to-be-deleted block management table 1149 includes a pool number column 11491, an LDEV number column 11492, a start address column 11493, and an end address column 11494.

[0068] The pool number column 11491, the LDEV number column 11492, the start address column 11493, and the end address column 11494 each has recorded therein the pool number of a pool having a block that is already released from allocation to an LU to maintain storage data to be deleted, an LDEV number, the LBA of the start block of the above blocks, and the LBA of the end block of the above blocks, respectively.

[0069] <General Outline of Encryption Control Process in the Present Embodiment>

An example of a data encryption control process (virtual volume encryption control process) carried out by the storage system 1 of the present embodiment will then be described referring to Figs. 15A to 15C. The relation between a virtual volume and a pool will be described before the description of the encryption control process.

[0070] As described above, a virtual volume is a virtual logical volume that is provided to the host computer 30 as a data storage area. A pool area is a group of LDEVs each functioning as a unit logical storage area, and is configured with a multiplicity of blocks. Fig. 16 diagrammatically depicts the relation between a physical storage area, an LDEV, and a virtual volume (virtual storage area.)

[0071] When the storage apparatus 10 receives a request to write data to a virtual volume from the host computer 30 and a need to newly store data in the virtual volume arises, the control program 1141 allocates an unallocated block included in a pool area to the virtual volume, and newly stores data on the write request in the block allocated to the virtual volume. The corresponding relation between a block allocation destination (range of LBA of each LU) and a block allocation source (range of LBA of each LDEV) is managed on the allocated block management table 1147.

[0072] Whether data stored in a virtual volume is to be encrypted or not is determined by an encryption attribute that is set on a pool linked to the virtual volume. Specifically,

when data is stored in a virtual volume linked to a pool with an encryption attribute "cipher" recorded in the encryption attribute column 11465 on the pool management table 1146, the data to be written in is encrypted. When data is stored in a virtual volume linked to a pool with an encryption attribute "plain text" recorded on the table, the data is stored in the form of plain text without being encrypted.

- [0073] A case is assumed where a virtual volume already containing plain text data is encrypted when determining whether or not encryption is to be performed not in units of virtual volumes recognized by the host computer 30 but in units of logical storage areas, such as in units of pools, recognized by the storage apparatus 10. In this case, it is necessary to encrypt data in all virtual volumes that share the same pool providing a block to the virtual volume to be encrypted. This results in encrypting data that does not need to be encrypted, thus putting unnecessary load on the storage system 1.
- [0074] Figs. 15A to 15C schematically depict a process of this embodiment of encrypting only the data stored in a specific virtual volume. Figs. 15A to 15C depict examples of encrypting only the data stored in a virtual volume 1.
- [0075] As shown in Fig. 15A, when the storage apparatus 10 receives a command to encrypt data stored in the virtual volume 1 from the management computer 20, the control program 1140 stored in the SM 114 of the disk control unit 11 of the storage apparatus 10 is executed to retrieve a pool meeting a encryption condition among pools managed by the storage apparatus 10. When the presence of the pool is judged, the pool is determined to be a data destination pool.
- [0076] As shown in Fig. 15B, the control program 1140 is executed to read data from the virtual volume 1 that is stored in a pool 1. The data read is encrypted by the encryption/decryption control part 11404 of the control program 1140, and the encrypted data is then stored in the transfer target pool by the data transfer processing part 11407. The above data encryption and transfer process is carried out by the control program 1140 on all blocks allocated to the virtual volume 1.
- [0077] Finally, as shown in Fig. 15C, plain text data allocated to the virtual volume 1 that is stored in the pool 1 is deleted, and a block from which the data is deleted is released as an unallocated block.
- [0078] <Data Encryption Control Process Flow of This Embodiment>
- An example of a process flow that is executed when the storage apparatus 10 receives a data encryption instruction for a specific virtual volume from the management computer 20 will then be described referring to Fig. 17. This process flow is carried out as the CPU 112 of the disk control unit 11 executes the control program 1140 stored in the SM 114 in the disk control unit 11 of the storage apparatus 10. A process executed mainly by the control program 1140 or a function unit included therein is realized as the CPU 112 executes the control program 1140. In the following

process flow, the character "S" denotes step.

- [0079] The control program 1140 of the storage apparatus 10 receives an encryption instruction from the management computer 20 (S171). An encryption condition includes items such as an encryption algorithm to be used, an encryption method including key length, etc., and specification on whether encrypted data is to be stored in an LDEV of the storage apparatus 10 or in an LDEV of the external storage apparatus 40. The encryption/decryption control part 11404 of the control program 1140 acquires the encryption condition from the received encryption instruction.
- [0080] The control program 1140 then refers to the pool management table 1146, and retrieves a pool that secures a memory capacity necessary for storing encrypted data and that meets the encryption condition, from pools with the encryption attribute 11465 set as "cipher" (S172).
- [0081] The encryption/decryption control part 11404 of the control program 1140 judges whether a pool meeting the encryption condition is present, based on records in the pool use ratio column 11464, the encryption attribute column 11465, and the encryption method column 11466 of the pool management table 1146 (S173). When the presence of a pool meeting the encryption condition is judged (S173: Yes), a data transfer process at S178 is executed to end the process flow. The data transfer process at S178 will be described later with reference to Fig. 18.
- [0082] When the presence of a pool meeting the encryption condition is not shown at S173 (S173: No), the encryption/decryption control part 11404 refers to the parity group management table 1141, the external volume group management table 1142, the LDEV management table 1143, and the external LDEV management table 1144, and retrieves a parity group or an external volume group on which an LDEV is not created (S174).
- [0083] The encryption/decryption control part 11404 checks to see if a parity group or an external volume group not registered in the LDEV management table 1143 or the external LDEV management table 1144 is present, and determines whether a parity group or an external volume group on which an LDEV is not created is present (S175).
- [0084] When judging that a parity group or an external volume group on which an LDEV is not created is present (S175: Yes), the encryption/decryption control part 11404 creates LDEVs formatted for encrypted (S176), and configures a pool composed of the created LDEVs (S177). The data transfer process at S178 is then executed in the same manner as in the case of Yes at S173 to end the process flow.
- [0085] When judging that no parity group or an external volume group on which an LDEV is not created is present (S175: No), the encryption/decryption control part 11404 transmits information indicative of the incapability of encrypting a virtual volume to be encrypted according to the encryption instruction from the management computer 20

under the specified condition, to the management computer 20, after which the process flow ends (S179).

[0086] According to the above configuration, an encrypted state of stored data can be changed in virtual volumes used by the host computer 30 without changing the encrypted state of stored data in units of parity groups or in units of external volume groups.

[0087] Even if a pool matching an encryption condition is not present, a pool matching a desired encryption condition can be configured from a parity group or an external volume group.

[0088] An example of a detailed process flow of a data transfer process step (S178) in the process flow of Fig. 17 will then be described referring to Figs. 18A and 18B.

[0089] The encryption/decryption control part 11404 of the control program 1140 judges whether encryption has been completed for all blocks allocated to a to-be-encrypted virtual volume (S1801). When judging that encryption has not been completed (S1801: No), the encryption/decryption control part 11404 refers to the allocation block management table 1147 to acquire the LDEV number 11474 of an LDEV having a block allocated to the LUN 11471 of the to-be-encrypted virtual volume and the start address 11475 and end address 11476 of the block (S1802).

[0090] The encryption/decryption control part 11404 of the control program 1140 then refers to the unallocated block management table 1148 to judge whether an LDEV which has a block not allocated to any virtual volume is present in an encrypted data storage destination pool judged at S173 or S177 in the process flow of Fig. 17 (S1803). When judging that the LDEV is present (S1803: Yes), the encryption/decryption control part 11404 acquires the LDEV number 11482 of the LDEV and the start address 11483 and the end address 11484 of the block (S1804).

[0091] When judging that an LDEV having a block not allocated to any virtual volume is not present (S1803: No), the encryption/decryption control part 11404, for example, sends an error notice through the management computer 20 to end the process flow (S1812).

[0092] The encryption/decryption control part 11404 of the control program 1140 then reads out stored data from the block specified by the LDEV number 11474, the start address 11475, and the end address 11476 that are acquired at step S1802, and encrypts the read data (S1805).

[0093] The encryption/decryption control part 11404 of the control program 1140 then stores the encrypted data in the block specified by the LDEV number 11482, the start address 11483, and the end address 11484 that are acquired at step S1803 (S1806).

[0094] The data transfer processing part 11407 of the control program 1140 then registers the LDEV number 11474 and the start address 11475 and end address 11476 of the

block acquired at S1802, to the scheduled to-be-deleted block management table 1149, and replaces the LDEV number column 11474, the start address column 11475, and end address column 11476, to which entries of the LDEV number 11474 and the start address 11475 and end address 11476 of the block that are acquired at S1802 of the allocation block management table are registered, with the LDEV number 11482 and the start address 11483 and end address 11484 of the block that are acquired at S1803. In addition, the data transfer processing part 11407 deletes registered entries of the LDEV number 11482 and the start address 11483 and end address 11484 of the block that are acquired at S1804, from the unallocated block management table 1148 (S1807).

- [0095] The above process from S1802 to S1807 is carried out repeatedly on all blocks allocated to the to-be-encrypted virtual volume (S1801: No). When the process of these steps on all blocks is judged to have completed (S1801: Yes), the process flow proceeds to step S1808.
- [0096] The data transfer processing part 11407 of the control program 1140 judges whether releasing of all blocks allocated to the to-be-encrypted virtual volume has been completed (S1808). When judging that releasing of all blocks has not been completed (S1808: No), that is, when referring to the scheduled-to-be-deleted block management table 1149 to judge that an entry remains on the scheduled-to-be-deleted block management table 1149, the data transfer processing part 11407 acquires the LDEV number 11492, the start address 11493, and the end address 11494 of a block required to be deleted remaining as the entry (S1809).
- [0097] The data transfer processing part 11407 then deletes data stored in the block specified by the LDEV number, the start address, and the end address that are acquired at S1809 (S1810).
- [0098] The data transfer processing part 11407 then deletes the registered entry of the LDEV number, the start address, and the end address that are acquired at S1809 from the scheduled-to-be-deleted block management table 1149, and registers the LDEV number, the start address, and the end address that are acquired at S1809 in the unallocated block management table 1148 (S1811).
- [0099] The process from S1808 to S1811 is carried out repeatedly on all blocks allocated to the to-be-encrypted virtual volume (S1808: No). When the completion of the process of these steps on all blocks is judged (S1808: Yes), the process flow comes to an end.
- [0100] The above configuration allows securing data safety by complete deletion of the plain text data and the effective use of a block from which data is deleted as a storage area for other data.
- [0101] <User Interface of Management Computer 20>
A management screen serving as a user interface that can be displayed on the output device 1005 of the management computer 20 of Fig. 1 will then be described. Figs.

19A to 19C are diagrams of display examples of a user interface (screen display) that is used by an administrator of the storage system 1 of this embodiment to transmit an encryption command to a virtual volume of the storage apparatus 10 from the management computer 20. These user interface screens are displayed, for example, on the output device 1005 that is a liquid crystal monitor as the management program 201 of the management computer 20 is executed by the CPU 1001.

- [0102] Fig. 19A is a diagram of a display example of a to-be-encrypted volume selection screen 60 for specifying a virtual volume (LU) to be encrypted.
- [0103] A plain text volume list 61 is displayed on the to-be-encrypted volume setting screen 60. The plain text volume list 61 includes, for example, a virtual volume number that is an identification code for a virtual volume recognized by the host management computer 30, the storage capacity of the virtual volume, the pool number of a pool corresponding to the virtual volume, the current encryption attribute of the virtual volume, and a check box for selecting a to-be-encrypted virtual volume.
- [0104] The plain text volume list 61 displays a list of virtual volumes linked to a pool with an encryption attribute of plain text out of virtual volumes provided by the storage apparatus 10.
- [0105] When encrypting data stored in a virtual volume, the storage administrator selects a virtual volume to be encrypted from the list 61 using the check box, and clicks an OK button 62. A cancel button 63 is operated when a selection process on the screen is to be canceled.
- [0106] Fig. 19B is a diagram of a display example of an encryption condition specifying screen 70 that is displayed when the OK button 62 is operated on the to-be-encrypted volume setting screen 60 of Fig. 19A.
- [0107] An encryption condition 71 is displayed on the encryption condition specifying screen 70. The encryption condition 71 enables the administrator to specify a condition for encryption including a encryption method, a key length, and an encrypted data storage area that are applied when a virtual volume specified on the to-be-encrypted volume setting screen 60 is encrypted. The storage administrator specifies the encryption condition on the screen of encryption condition 71, and clicks an OK button 72. A cancel button 73 is operated when a specifying process on the screen is to be canceled.
- [0108] Fig. 19C is a diagram of a display example of a to-be-encrypted volume/pool combination determining screen 80 that is displayed when the OK button 72 is clicked on the encryption condition specifying screen 70. A to-be-encryption volume/pool combination list 81 is displayed on the to-be-encrypted volume/pool combination determining screen 80.
- [0109] The to-be-encrypted volume/pool combination list 81 displays combinations of

virtual volumes that are selected by the storage administrator to be encrypted on the to-be-encrypted volume setting screen 60 and pools meeting a encryption condition that are specified on the encryption condition specifying screen 70. In the example of Fig. 19C, the list 81 displays the virtual volume number of a selected virtual volume, the use capacity of the virtual volume, and the pool number of a pool currently linked to the virtual volume, together with the pool number of a pool linked to the virtual volume after encryption, the storage capacity of the post-encryption pool, and the capacity use ratio of the post-encryption pool.

- [0110] The storage administrator checks a combination of a to-be-encrypted volume and a post-encryption pool, and clicks an encryption execution button 82 when determining the combination to be appropriate. As a result, an encryption process command is transmitted from the management computer 20 to the disk control unit 11 of the storage apparatus 10, which starts the control program 1140 of the SM 114 to execute encryption of a to-be-encrypted virtual volume.
- [0111] When the storage administrator determines that an appropriate combination is not displayed, the storage administrator may be allowed to set a combination of a to-be-encrypted volume and a pool through manual input on the screen 80. When a plurality of candidates of pools to be combined with a single to-be-encrypted virtual volume are retrieved, the storage administrator may be allowed to select a pool determined by the administrator to be appropriate out of the candidates of pools.
- [0112] According to the embodiment as described above, only the data stored in a specific virtual volume can selectively be encrypted. While only the case of encrypting plain text data is described in this embodiment, the configuration described in this embodiment applies not only to the case of encrypting plain text data, but also to a case of decrypting encrypted data and to a case of changing a encryption key to encrypted data. Data storage states may be classified in virtual volumes in accordance with an appropriate attribute other than data encryption.

Claims

- [1] A storage system comprising a storage apparatus having a storage control unit communicatively coupled to an external apparatus, forming a plurality of virtual storage areas each serving as a unit storage area used by the external apparatus as a data storing area, using a unit logical storage area selected among a plurality of unit logical storage areas provided by a physical storage medium, linking to each of the virtual storage areas, and any one of a plurality of attributes each representing a storage state of data stored in the virtual storage area, and maintaining the link wherein the storage control unit further includes a logical storage area management unit that manages the link of the virtual storage area and any one of the attributes to each of logical storage area groups each configured to include the unit logical storage area to maintain the link and manage the linking relation, wherein the logical storage area management unit, when receiving a command to change an attribute of any one of the virtual storage areas to a different attribute, determines presence or absence of the unit logical storage area that belongs to the logical storage area group linked to the changed different attribute and that is not yet allocated to any one of the virtual storage areas, and when determining the presence of the unit logical storage area that is not yet allocated to any one of the virtual storage areas, the logical storage area management unit links the unit logical storage area determined to be present to the virtual storage area, reads out data stored in the unit logical storage area linked to a virtual storage area subjected to the attribute change, and stores the read data in the unit logical storage area determined to be present in accordance with a storage state represented by the different attribute.
- [2] The storage system of claim 1, wherein the physical storage medium includes a plurality of physical disks, wherein the plurality of attributes includes an encryption attribute representing encryption of the data to be stored in the unit storage area, and a plain text attribute representing storage of the data to be stored in a form of plain text data, wherein the storage control unit configures a parity group as an RAID group organized with the physical disks, and keeps a corresponding relation between each of the parity group and the unit logical storage area and any one of the attributes, and wherein the logical storage area management unit maintains a corresponding relation

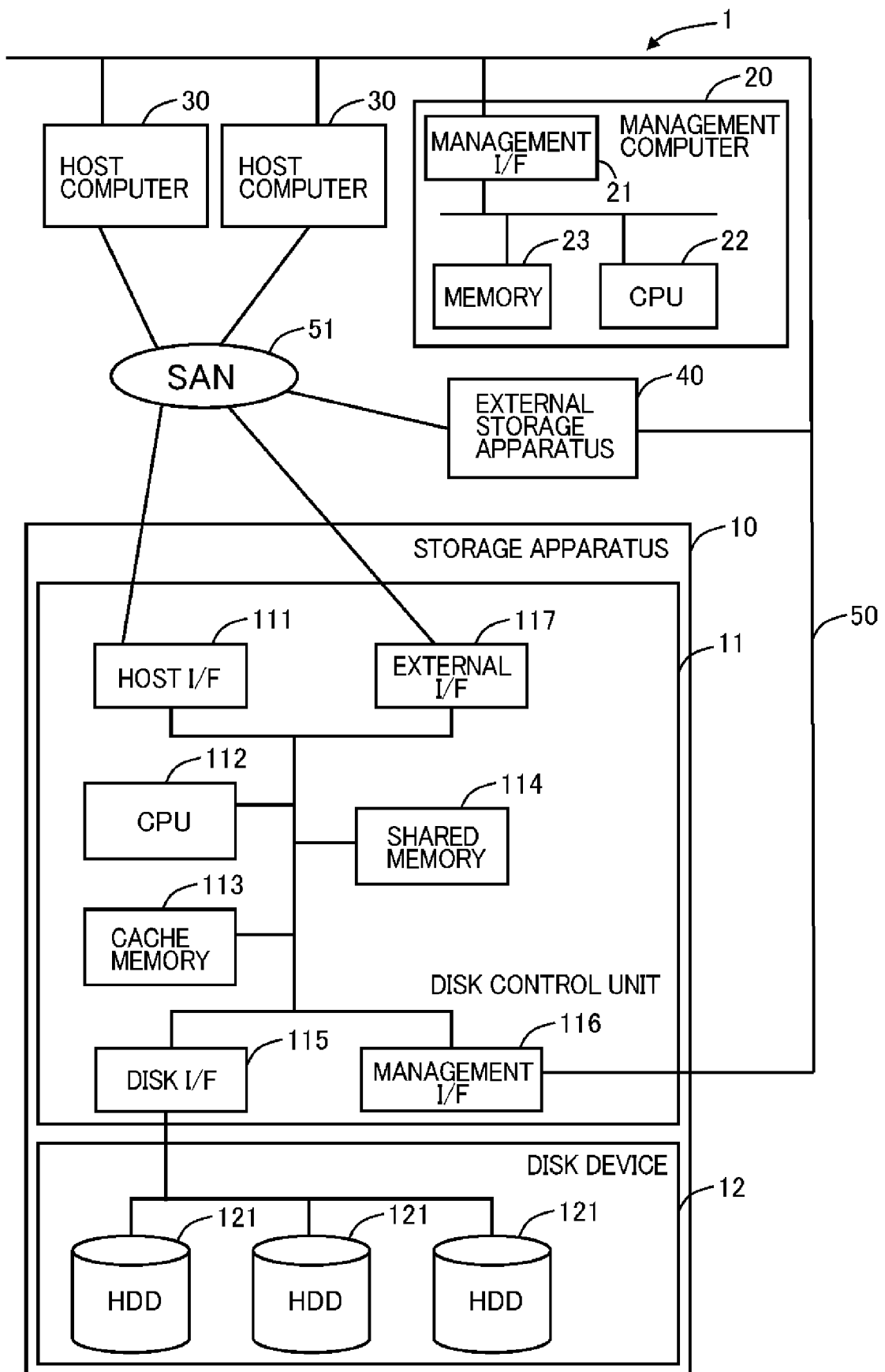
between the unit logical storage area, a pool area including each of the unit logical storage area, each pool area, and the attribute, the logical storage area management unit comprising: an encryption/decryption control part that when receiving a command to change an attribute of the virtual storage area, judges presence or absence of the pool area linked to the changed attribute, and that when judging the presence of the pool area, judges presence or absence of the unit storage area linked to the pool area judged to be present; and a data transfer processing part that when judging the presence of the unit storage area linked to the pool area judged to be present, links the unit storage area judged to be present to the virtual storage area, reads out data stored in the unit logical storage area linked to the virtual storage area subjected to the attribute change, and stores the read data in the unit logical storage area judged to be present in accordance with a storage state represented by the different attribute, the data transfer processing part judges presence or absence of the parity group not linked to the unit logical storage area when judging the absence of the pool area linked to the changed attribute, and newly creating the pool area using the unit storage area included in the parity group to execute the attribute change process when the presence of the pool area linked to the changed attribute is judged.

- [3] The storage system of claim 1, wherein when the attribute change is carried out, the logical storage area management part cancels a corresponding link between the unit logical storage area having been linked to an attribute before the attribute change and the virtual storage area subjected to the attribute change, deletes the data stored in the unit logical storage area in which the corresponding link has been canceled, and links the unit storage area released from the corresponding link to the logical storage area group linked to an attribute before the attribute change to maintain the link.
- [4] The storage system of claim 1, wherein the plurality of attributes includes an encryption attribute representing encryption of the data to be stored in the unit storage area, and a plain text attribute representing storing of the data to be stored in a form of plain text data.
- [5] The storage system of claim 1, further comprising an external storage apparatus that includes a physical storage medium to provide a plurality of unit logical storage areas created from the physical storage mediums, wherein the storage control unit of the storage apparatus is communicatively coupled to the external storage apparatus, links any one of the attributes to each of the logical storage area group including the unit storage area of the external storage

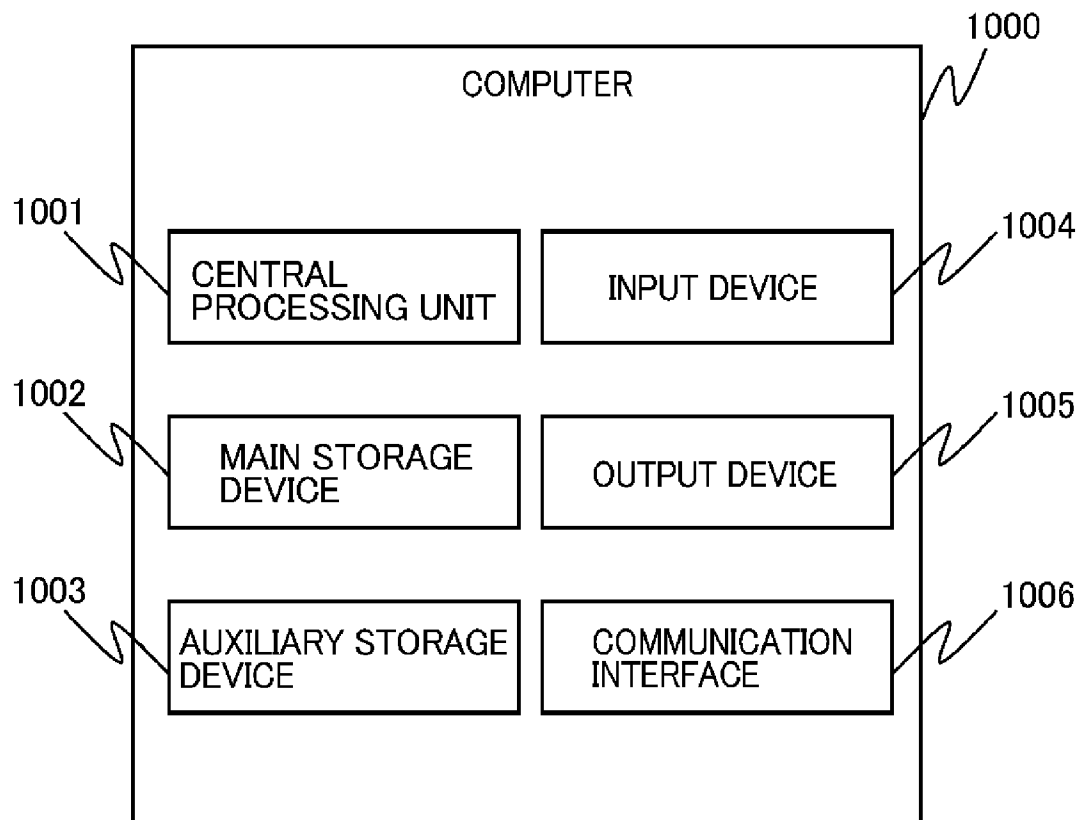
- apparatus to maintain the link, and provides the logical storage area provided by the external storage apparatus to the external apparatus.
- [6] The storage system of claim 1, further comprising a management computer communicatively coupled to the storage apparatus 40, wherein the management computer generates information for commanding the storage control unit of the storage apparatus to change an attribute of the virtual storage area, based on an input attribute change condition, and transmits the information to the storage apparatus.
- [7] The storage system of claim 6, wherein the management computer outputs a user interface screen for each of the virtual storage area, the user interface screen displaying a storage capacity of the virtual storage area, the logical storage area group linked to the virtual storage area, and any one of the attributes linked to the virtual storage area.
- [8] The storage system of claim 6, wherein when encrypting data to be stored in the virtual storage area is set as the attribute, the management computer outputs a user interface screen for selecting an encryption method used for the encryption.
- [9] The storage system of claim 6, wherein when receiving a command to change an attribute set for the virtual storage area to an encryption attribute representing encrypting of data to be stored in the virtual storage area, the management computer outputs a user interface screen for each of the virtual storage area provided by the storage apparatus, the user interface screen displaying at least a storage capacity of the virtual storage area, the logical storage area group linked to the virtual storage area, and the logical storage area group to which the virtual storage area is to be linked when an encryption attribute is set for the virtual storage area.
- [10] A method of operating a storage system comprising a storage apparatus having a storage control unit communicatively coupled to an external apparatus, forming a plurality of virtual storage areas each serving as a unit storage area used by the external apparatus as a data storing area, using a unit logical storage area selected among a plurality of unit logical storage areas provided by a physical storage medium, linking any one of a plurality of attributes each representing a stored state of data stored in the virtual storage area, to each of the virtual storage areas to maintain the link, the storage control unit including a logical storage area management unit that manages the links of the virtual storage area and any one of the attributes to each

of a plurality of logical storage area groups that is a logical storage area including the unit logical storage area to maintain the link and manage the linking relation, wherein
the logical storage area management unit
when receiving a command to change an attribute of any one of the virtual storage areas to a different attribute, determines presence or absence of the unit logical storage area that belongs to the logical storage area group linked to the changed different attribute and that is not yet allocated to any one of the virtual storage areas, and wherein
when determining the presence of the unit logical storage area that is not yet allocated to any one of the virtual storage areas, the logical storage area management unit links the unit logical storage area determined to be present to the virtual storage area, reads out data stored in the unit logical storage area linked to a virtual storage area subjected to the attribute change, and stores the read data in the unit logical storage area determined to be present in accordance with a storage state represented by the different attribute.

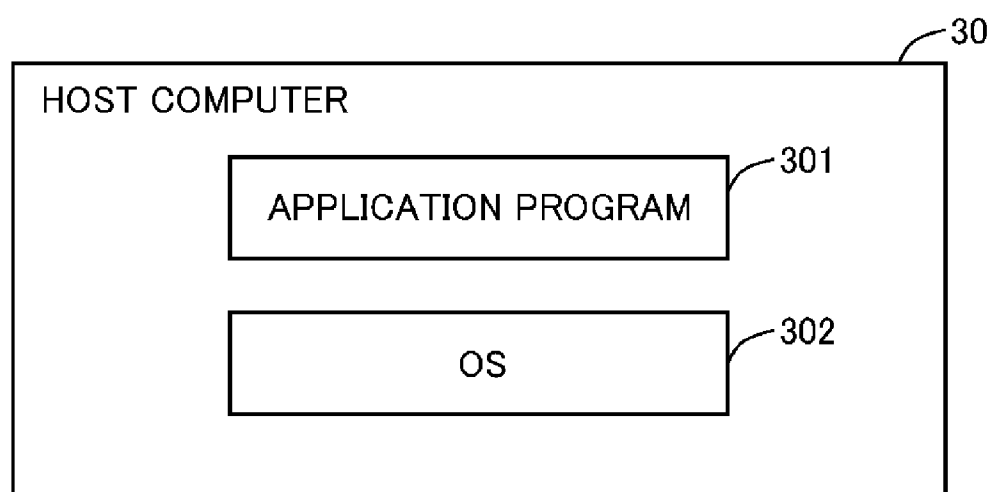
[Fig. 1]



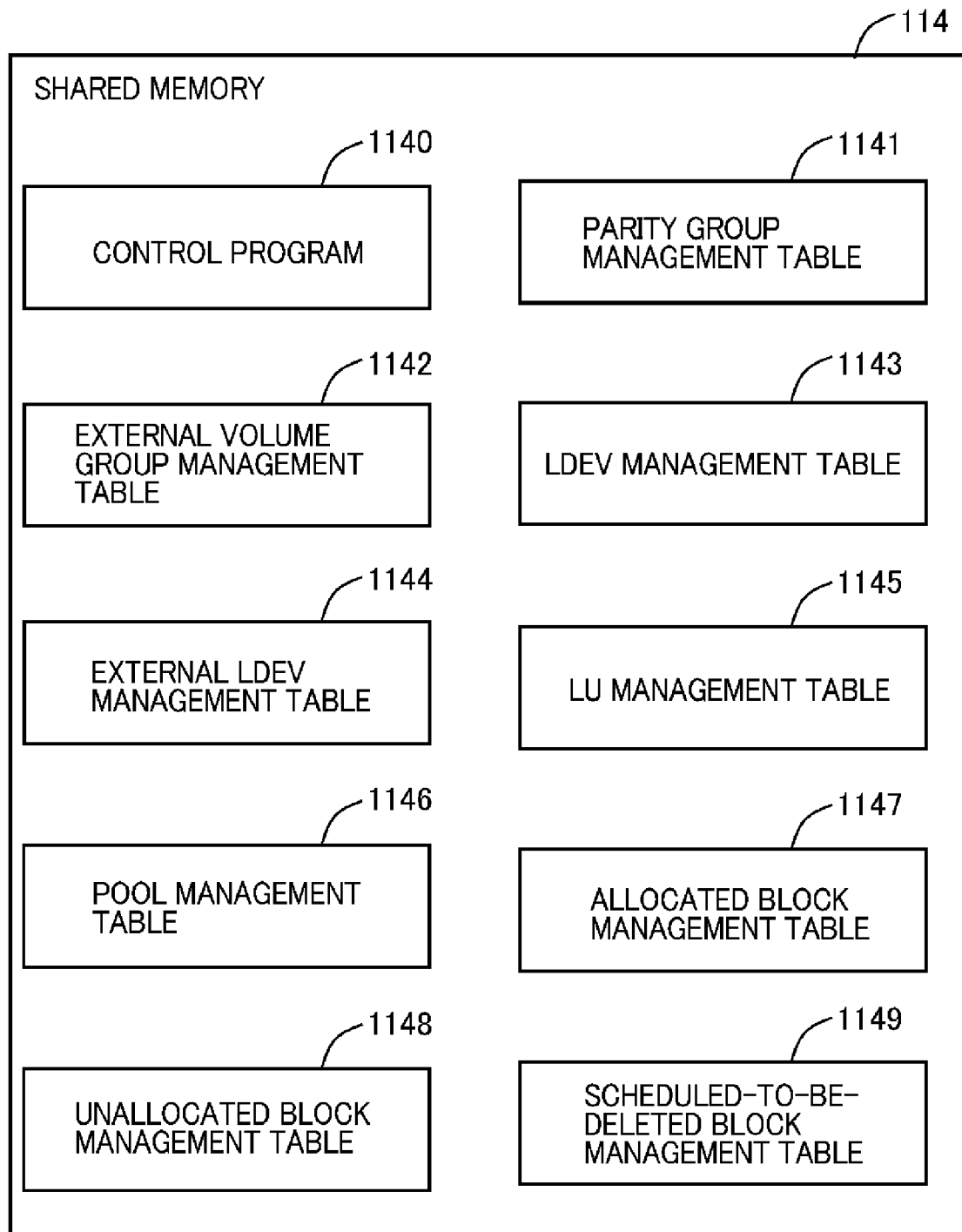
[Fig. 2]



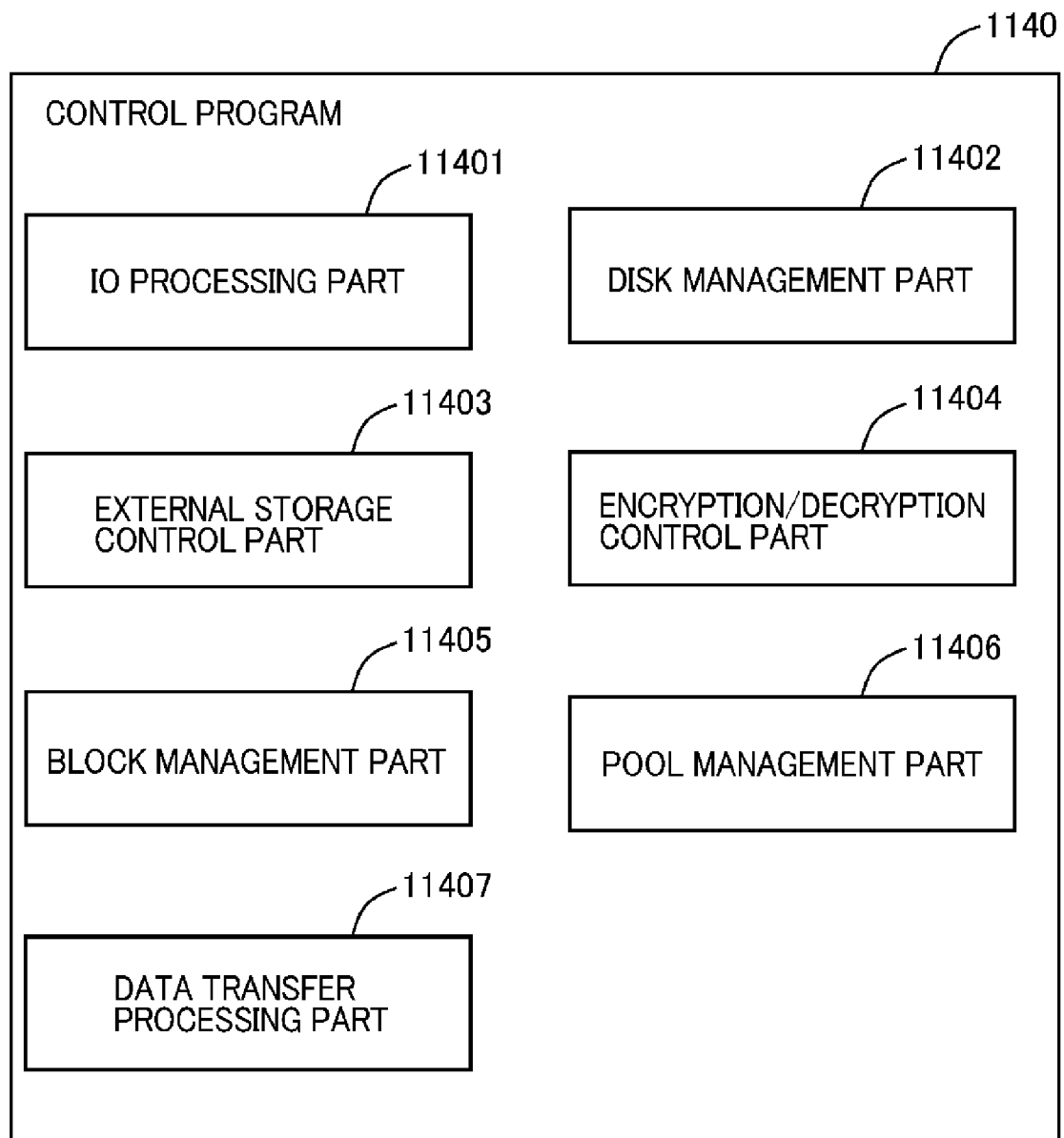
[Fig. 3]



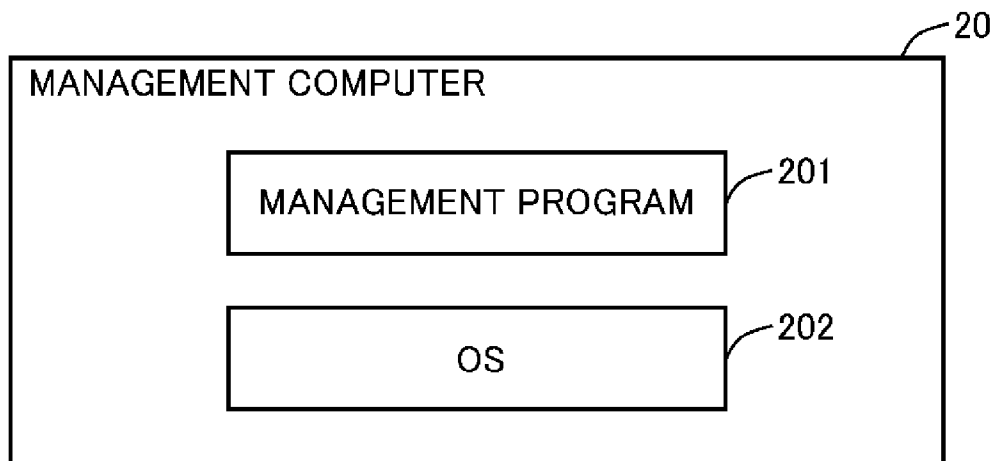
[Fig. 4A]



[Fig. 4B]



[Fig. 5]



[Fig. 6]

PARITY GROUP MANAGEMENT TABLE 1141

11411 PARITY GROUP#	11412 DISK#	11413 RAID LEVEL	11414 ENCRYPTION ATTRIBUTE	11415 KEY	11416 ENCRYPTION METHOD
1	1, 2, 3, 4	5	PLAIN TEXT		
2	5, 6, 7, 8	5	CIPHER	0x1234 5678	AES- CBC- 256
...	...	...	...	...	...

[Fig. 7]

EXTERNAL VOLUME GROUP MANAGEMENT TABLE 1142

11421 EXTERNAL VOLUME GROUP#	11422 WWN	11423 LUN	11424 ENCRYPTION ATTRIBUTE	11425 KEY	11426 ENCRYPTION METHOD
1	12:34:56: 78:9a:bc	1	CIPHER	0x987 65432	AES- ECB- 256
2	98:75:54: 32:1c:ba	2	PLAIN TEXT		
...	...	...	...	...	...

[Fig. 8]

LDEV MANAGEMENT TABLE 1143

11431 PARITY GROUP#	11432 LDEV#	11433 START ADDRESS	11434 END ADDRESS
1	1	1	200
1	2	201	400
...	...	...	...
2	15	1	200
2	16	201	400
...	...	...	...

[Fig. 9]

EXTERNAL LDEV MANAGEMENT TABLE 1144

EXTERNAL VOLUME GROUP#	LDEV#	START ADDRESS	END ADDRESS
1	101	1	200
1	102	201	400
...	...	...	...
2	115	1	200
2	116	201	400
...	...	...	...

[Fig. 10]

LU MANAGEMENT TABLE 1145

VIRTUAL VOLUME#	WWN	LUN	CAPACITY	POOL#
1	01:23:45: 67:89	0	10G	1
2	09:87:65: 43:21	1	20G	1
...	...	...	...	...

[Fig. 11]

POOL MANAGEMENT TABLE 1146

POOL#	LDEV#	POOL CAPACITY	POOL USE RATIO	ENCRYPTION ATTRIBUTE	ENCRYPTION METHOD
1	100, 110, 120, 130	200G	40%	CIPHER	AES-CBC-256
2	200, 210, 220, 230	150G	28%	PLAIN TEXT	
3	300, 310, 320, 330	200G	20%	CIPHER	AES-ECB-256
...	...	...	...	...	...

[Fig. 12]

ALLOCATED BLOCK MANAGEMENT TABLE 1147

LUN	START ADDRESS	END ADDRESS	LDEV #	START ADDRESS	END ADDRESS
1	1	10	100	1	10
1	11	20	110	1	10
...	...	...	...	...	...
2	1	10	200	1	10
...	...	...	...	...	...

[Fig. 13]

UNALLOCATED BLOCK MANAGEMENT TABLE 1148

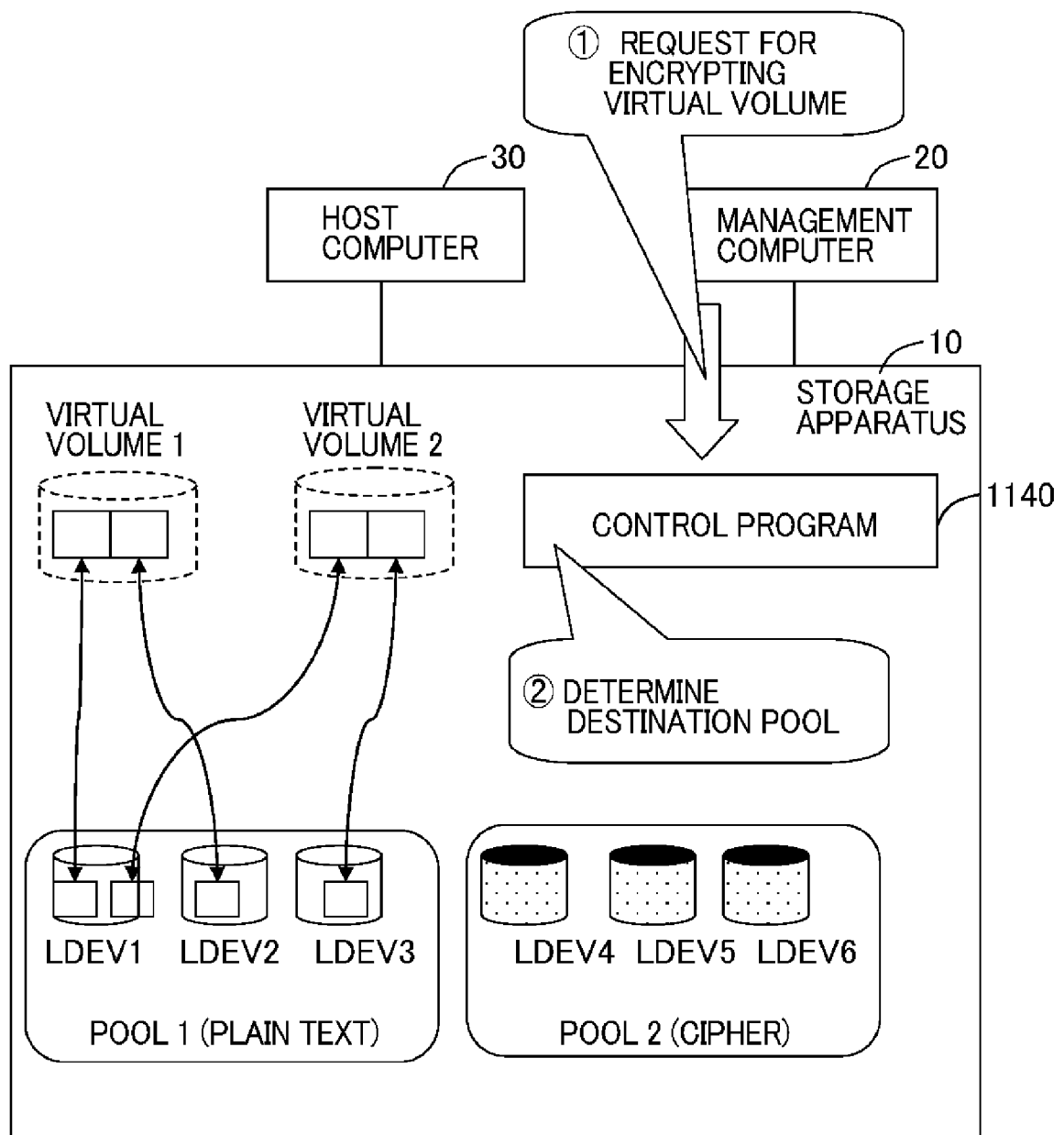
POOL#	LDEV#	START ADDRESS	END ADDRESS
1	100	11	200
1	110	11	200
...	...	...	...
2	200	1	200
2	200	211	280

[Fig. 14]

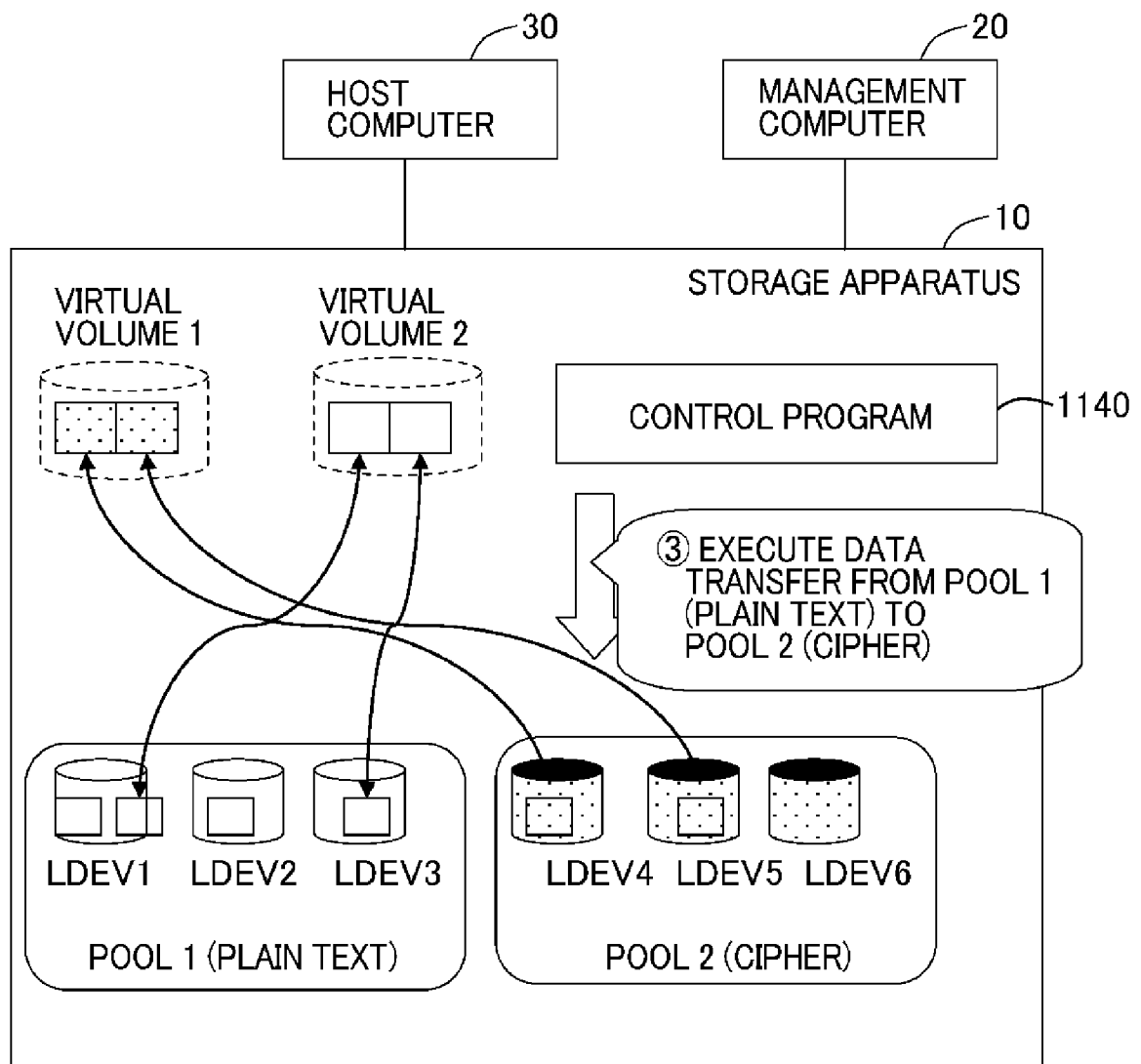
SCHEDULED-TO-BE-DELETED BLOCK MANAGEMENT TABLE 1149

POOL#	LDEV#	START ADDRESS	END ADDRESS
1	100	41	50
1	100	61	70
...	...	...	...
2	200	11	20

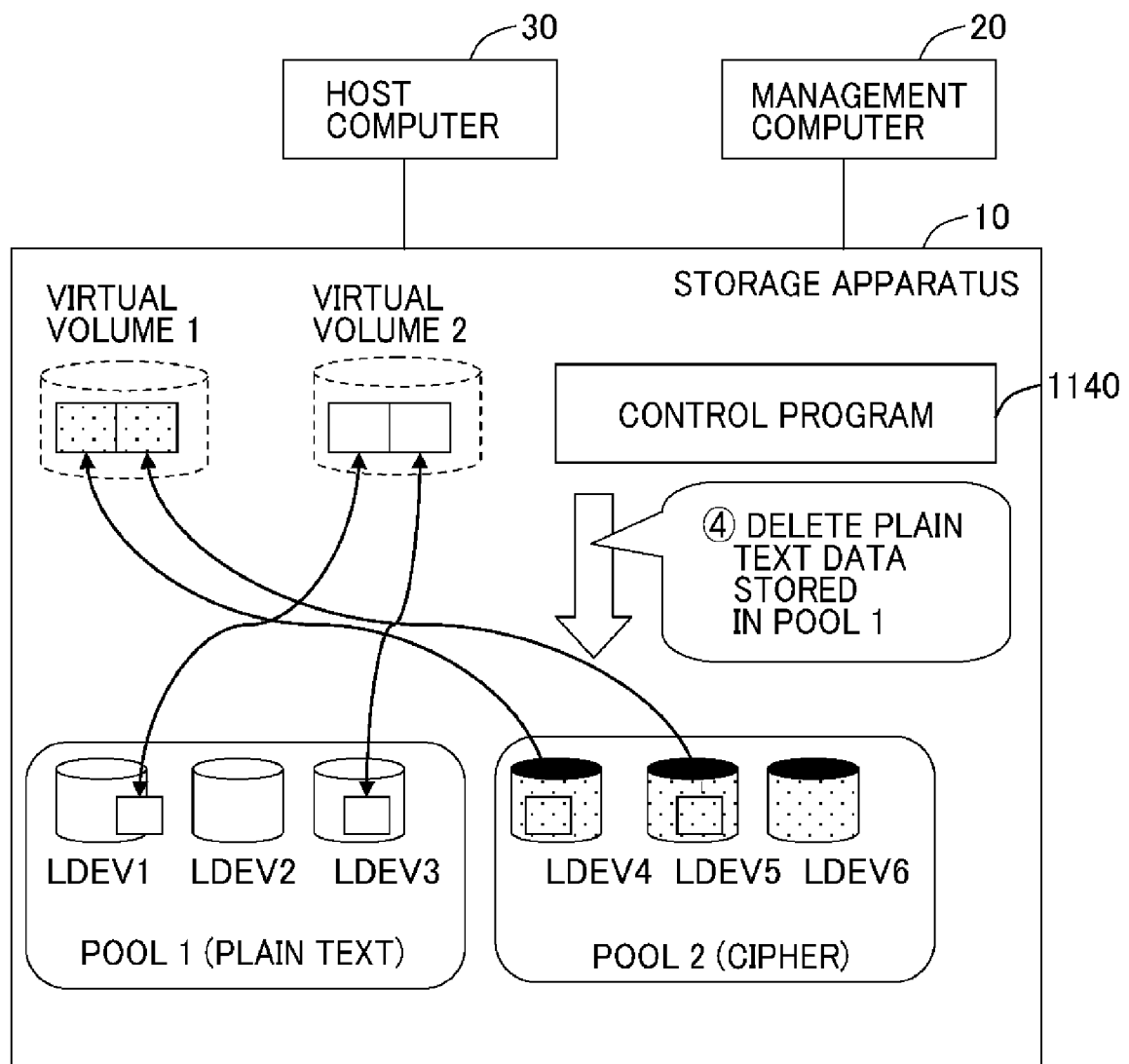
[Fig. 15A]



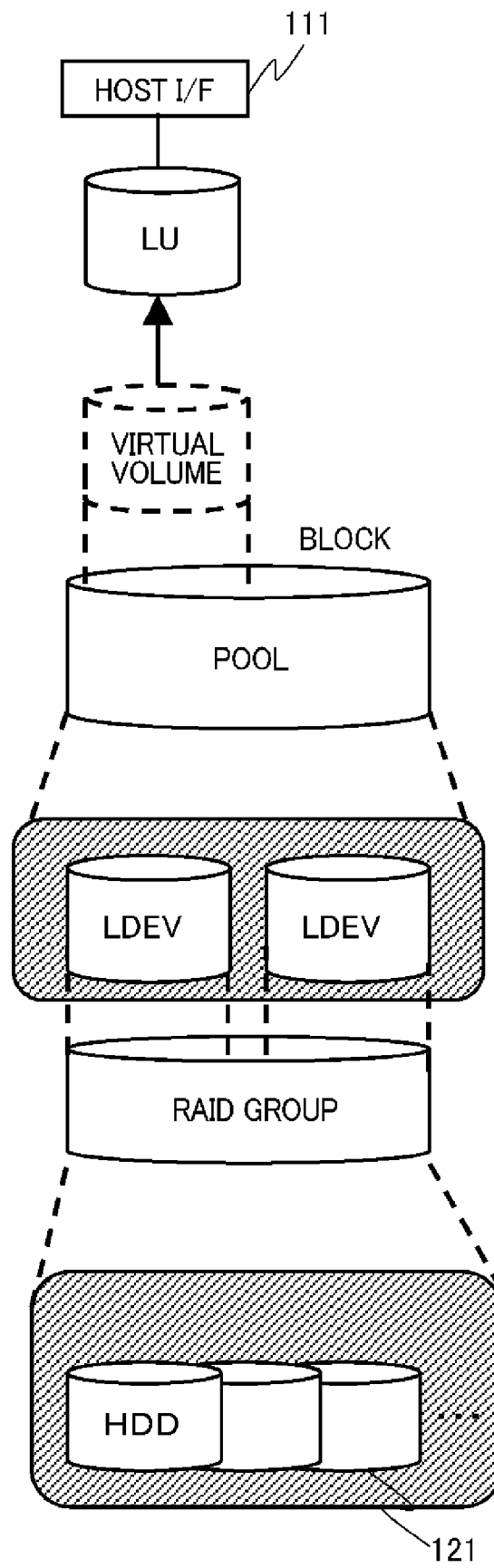
[Fig. 15B]



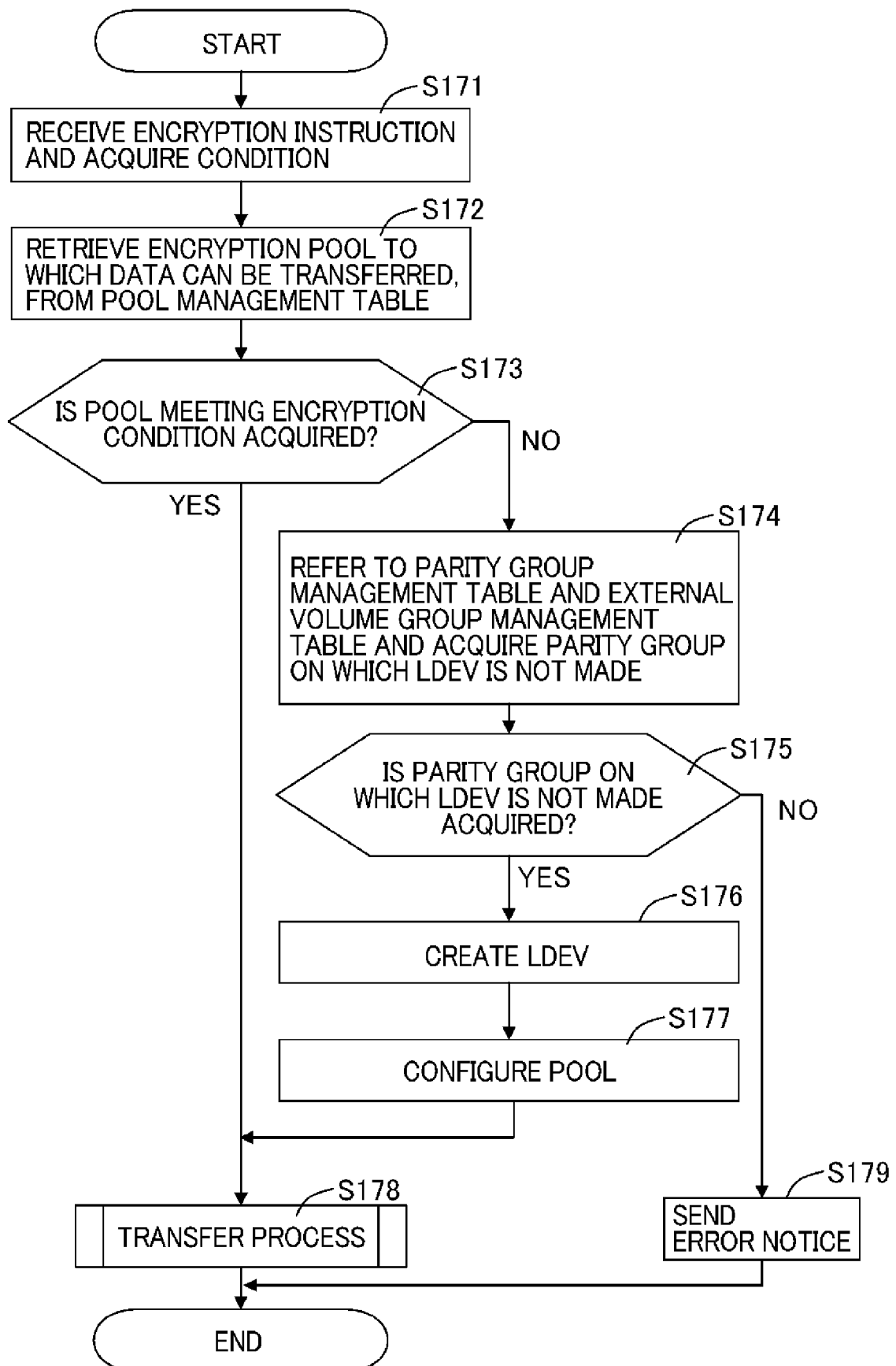
[Fig. 15C]



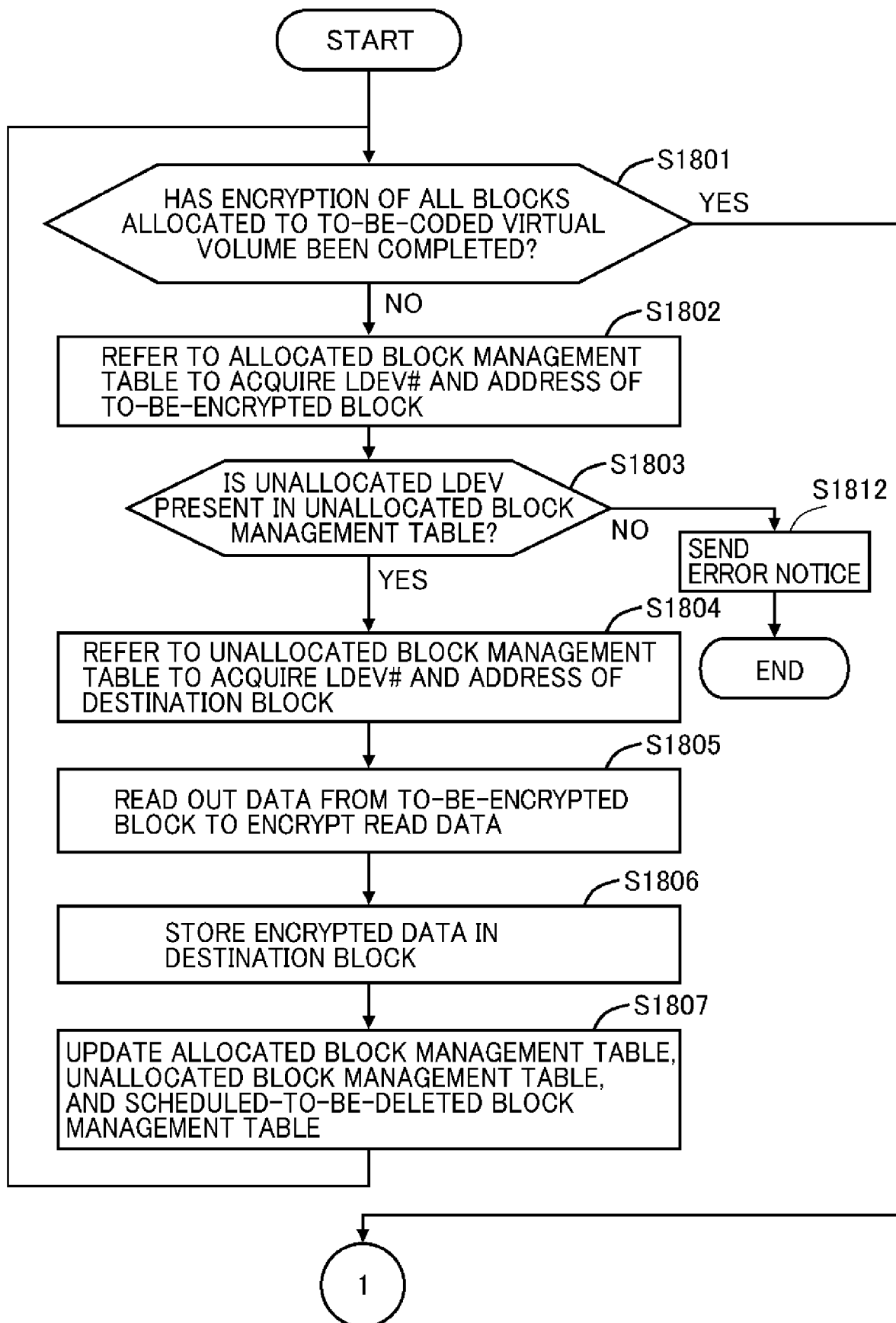
[Fig. 16]



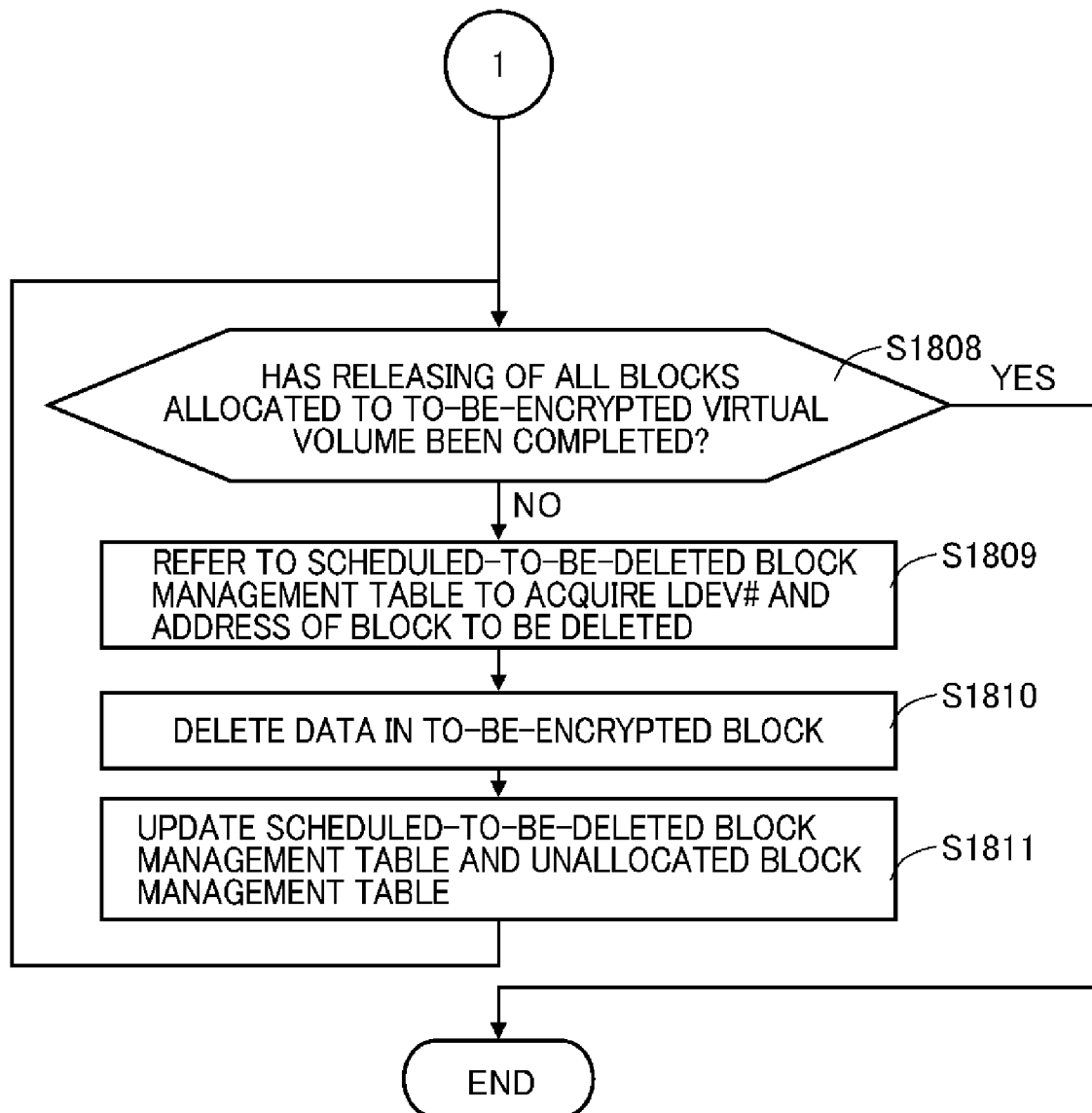
[Fig. 17]



[Fig. 18A]



[Fig. 18B]



[Fig. 19A]

60

SELECTING TO-BE-ENCRYPTED VOLUME

PLAIN TEXT VOLUME LIST

CHECK BOX	VIRTUAL VOLUME#	VIRTUAL VOLUME CAPACITY	POOL#	ENCRYPTION ATTRIBUTE
☒	1	10G	1	PLAIN TEXT
☐	2	20G	1	PLAIN TEXT
☒	3	20G	1	PLAIN TEXT
☒	4	100G	1	PLAIN TEXT
...	...		...	...

61

△

▽

62

OK

63

CANCEL

[Fig. 19B]

70

SPECIFYING ENCRYPTION CONDITION

71

ENCRIPTION CONDITION

· ENCRIPTION METHOD

☒ AES - CBC ☐ AES - ECB ☐ NOT SPECIFIED

· KEY LENGTH

☐ 128bit ☒ 256bit ☐ NOT SPECIFIED

· ENCRYPTED DATA STORAGE PLACE

☒ INTERNAL VOLUME ☐ EXTERNAL VOLUME ☐ NOT SPECIFIED

72 73

OK Cancel

[Fig. 19C]

80

DETERMINING TO-BE-ENCRYPTED VOLUME/POOL COMBINATION

TO-BE-ENCRYPTED VOLUME/POOL COMBINATION LIST

81

VIRTUAL VOLUME#	VIRTUAL VOLUME CAPACITY	CURRENT POOL#	ENCRYPTED POOL#	POOL CAPACITY	USE RATIO
1	10G	1	10	100G	8%
3	20G	1	10	100G	8%
4	100G	2	20	200G	0%
...		...			

△
▽

82

EXECUTE
ENCRYPTION

83

CANCEL

INTERNATIONAL SEARCH REPORT

International application No
PCT/JP2009/001483

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F3/06

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

B. FIELDS SEARCHED

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

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/143418 A1 (TAKAHASHI TORU [JP] ET AL) 29 June 2006 (2006-06-29)	1, 10
Y	paragraphs [0070], [0076] paragraphs [0115], [0119] paragraphs [0133], [0140] figure 1	2-9
Y	WO 2008/037741 A1 (IBM [US]; IBM UK [GB]; ASHER KAI ALAN GAHN [US]; CANNON DAVID MAXWELL) 3 April 2008 (2008-04-03) page 9, paragraph 2 - page 11, paragraph 2 figures 4,5	2-9
A	US 2008/263306 A1 (TANIZAWA AKINORI [JP]) 23 October 2008 (2008-10-23) paragraphs [0077] - [0094] paragraph [0135] - paragraph [0149] figures 2,3,8,9	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 document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

30 December 2009

Date of mailing of the international search report

08/01/2010

Name and mailing address of the ISA/

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

Authorized officer

Mazur, David

INTERNATIONAL SEARCH REPORT

International application No

PCT/JP2009/001483

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/113007 A1 (MURAYAMA KOICHI [JP] ET AL) 17 May 2007 (2007-05-17) paragraph [0116] - paragraph [0131] figure 11 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/JP2009/001483

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2006143418	A1	29-06-2006	NONE		
WO 2008037741	A1	03-04-2008	CN	101517589 A	26-08-2009
			US	2008082835 A1	03-04-2008
US 2008263306	A1	23-10-2008	JP	2008269090 A	06-11-2008
US 2007113007	A1	17-05-2007	JP	2007140728 A	07-06-2007