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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/006728 A1

(51) International Patent Classification:
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/CA2008/001218

(22) International Filing Date: 3 July 2008 (03.07.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/929,754 11 July 2007 (11.07.2007) US

(71) Applicant *(for all designated States except US)*: **MEMORY EXPERTS INTERNATIONAL INC.** [CA/CA]; 2321 Cohen Street, Montreal, Quebec H4R 2N7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PRIBADI, Kris** [CA/CA]; 50 Huron Road, Dollard des Ormeaux, Quebec, H9G 2C4 (CA). **HAMID, Laurence** [CA/CA]; 561 Brookridge Crescent, Ottawa, Ontario K4A 1Z3 (CA).

(74) Agent: **FREEDMAN, Gordon**; Freedman & Associates, 117 Centrepointe Drive, Suite 350, Nepean, Ontario K2G 5X3 (CA).

(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, 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 applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) **Title:** SECURING TEMPORARY DATA STORED IN NON-VOLATILE MEMORY USING VOLATILE MEMORY

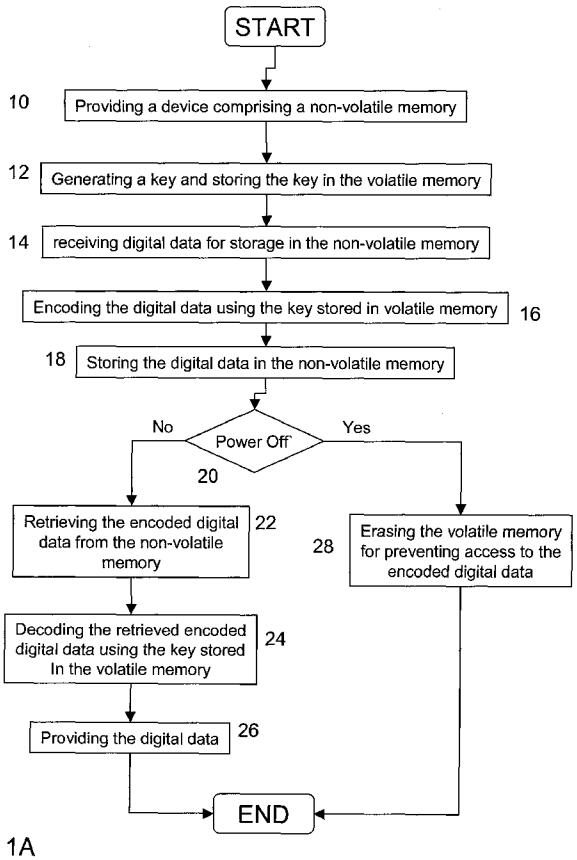

Fig. 1A

(57) **Abstract:** Temporary digital data received for storage in non-volatile memory are encoded using a key stored in volatile memory. The encoded digital data are then stored in the non-volatile memory. As long as there has been no interruption of supply of power to the volatile memory, the key is available enabling decoding of the encoded digital data stored in the non- volatile memory. Upon interruption of supply of power to the volatile memory the key is erased. Absent the key, access to the encoded digital data stored in the non-volatile memory is prevented.

WO 2009/006728 A1

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

SECURING TEMPORARY DATA STORED IN NON-VOLATILE MEMORY USING VOLATILE MEMORY

FIELD OF THE INVENTION

[001] The instant invention relates to the field of computer security and in particular to a method and system for securely storing temporary data stored in non-volatile memory.

BACKGROUND OF THE INVENTION

[002] Information theft has become a major concern for every organization. A misconception shared by many is that printers, copiers, and fax machines are benign office machines and no more of a security threat than a mechanical typewriter. A recent survey of IT professionals revealed that 47% believed that copiers and printers didn't contain non-volatile memory such as a hard drive. Additionally, 65% believed that copiers and printers presented little or no risk to data security.

[003] Since non-volatile memory such as disk-storage is substantially cheaper for data volumes than volatile memory such as RAM, modern copiers, printers, and fax machines often contain non-volatile memory in the form of hard drives similar to thc workstations, personal computers, and laptops. These devices automatically store on ve any digital data that are received or generated for printing, copying, or faxing, i.e. ntain sensitive data on the hard drive resulting in an often overlooked security risk. ata are easily accessed by removing the hard drive from the device, for example, during maintenance or when the device is powered down, and connecting the hard drive to a computer. In high security areas, for example, military installations, there is often a requirement that all data stored in non-volatile memory such as a hard drive be inaccessible. To fulfill this requirement, security personnel must remove each hard drive from each common area device after power-down, store the same in a secure location such as a safe, and reinstall the same prior to power-up of the devices. As is evident, this is an expensive and inefficient routine for securing data.

[004] Another security risk of non-volatile memory is that even when data have been "erased," it is still possible to recover and read the data. For example, data are recovered because only a

directory entry or a pointer to the data is often erased in erasing of data, because data compression or multi-bit coding techniques do not overwrite a substantial portion of the data, or because techniques exist for detecting residual elements of a magnetic pattern remaining on the disk after an overwrite has been used.

[005] It would be beneficial to overcome the drawbacks of the present technology and to increase data security in devices such as printers, copiers, and fax machines.

SUMMARY OF THE INVENTION

[006] It is, therefore, an object of aspects of the invention to provide a method and system for securing temporary data stored in non-volatile memory.

[007] In accordance with an aspect of the present invention there is provided a method comprising: providing a device comprising a non-volatile memory; receiving digital data for being stored in the non-volatile memory; prior to storing the digital data in the non-volatile memory, encoding the digital data using a key stored in a volatile memory that is supplied with power only when the device is in a powered-on condition, the volatile memory for being erased automatically upon interruption of supply of power thereto, the encoding for preventing access to the digital data in a non-encoded form absent the key; storing the encoded digital data in the non-volatile memory; and, subsequent to storing the encoded digital data in the non-volatile memory, erasing the key from the volatile memory.

[008] In accordance with an aspect of the present invention there is provided a system comprising: volatile memory for storing a key therein, the volatile memory for being erased upon interruption of supply of power thereto; a communication and output port; circuitry connected to the communication and output port, to the volatile memory and for being connected to non-volatile memory of a device, the circuitry for: receiving temporary digital data for storage in the non-volatile memory of the device; encoding the temporary digital data using the key stored in the volatile memory, the encoding for preventing access to the encoded temporary digital data absent the key, the key other than stored within non-volatile memory of the device; providing the encoded temporary digital data for storage in the non-volatile memory; retrieving the encoded temporary digital data from the non-volatile memory; decoding the retrieved encoded

temporary digital data using the key stored in the volatile memory; and, providing the temporary digital data.

[009] In accordance with an aspect of the present invention there is provided a computer readable storage medium having stored thereon executable commands for execution on a processor, the processor when executing the commands performing: one of generating a key and receiving a key for use in encoding; storing the key in volatile memory; receiving digital data for storage in non-volatile memory of a device; encoding the digital data using the key stored in the volatile memory, the encoding for preventing access to the encoded digital data in a non-encoded form absent the key, the key other than stored within non-volatile memory of the device; providing the encoded digital data for storage in the non-volatile memory; retrieving the encoded digital data from the non-volatile memory; decoding the retrieved encoded digital data using the key stored in the volatile memory; and, providing the digital data.

[0010] In accordance with an aspect of the present invention there is provided a method comprising: providing a device for processing digital data and comprising a queue, the queue comprising non-volatile memory; receiving digital data for being stored within the queue and processed by the device; ciphering the received digital data with a key to provide secure data, the key stored in volatile memory and for being erased when at least one of power is other than provided to the volatile memory and the received digital data has been ciphered; storing the secure data within the queue; retrieving the secure data from the queue; deciphering the secure data using the key stored in volatile memory; and processing the deciphered secure data..

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0012] Figure 1a is a simplified flow diagram of a method for securing data stored in non-volatile memory according to an embodiment of the instant invention;

[0013] Figure 1b is a simplified flow diagram of a method for securing data stored in non-volatile memory according to an embodiment of the instant invention;

[0014] Figure 2a is a simplified block diagram of a system according to an embodiment of the instant invention for implementing the methods shown in Figures 1a and 1b;

[0015] Figure 2b is a simplified block diagram of a system according to an embodiment of the instant invention for implementing the methods shown in Figures 1a and 1b;

[0016] Figure 2c is a simplified block diagram of a system according to an embodiment of the instant invention for implementing the methods shown in Figures 1a and 1b; and,

[0017] Figure 2d is a simplified block diagram of a system according to an embodiment of the instant invention for implementing the methods shown in Figures 1a and 1b.

DETAILED DESCRIPTION OF THE DRAWINGS

[0018] The following description is presented to enable a person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the scope of the invention. Thus, the present invention is not intended to be limited to the embodiments disclosed, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

[0019] Referring to Fig. 1a, shown is a simplified flow diagram of a method for securing data stored in non-volatile memory, according to an embodiment of the instant invention. For the sake of clarity, the method is described in connection with system 100, shown in Figs. 2a and 2b, for its implementation. For example, in a corporate network such as a Local Area Network (LAN), devices 120 and 122 comprising non-volatile memory 110 such as a hard drive are provided - 10 - and connected to a server 124, as shown in Fig. 2a. The devices 120 and 122 comprise, for example, workstations, printers, copiers, and, fax machines. As will become evident, the method and system for securing data stored in non-volatile memory is also implementable in device 130 provided - at 10 - for independent operation, as shown in Fig. 2b, such as, for example, a copier or fax machine comprising non-volatile memory for storing data for printing multiple copies or

sending multiple faxes. Alternatively, the method is implemented using one of systems 200 and 300 of Figs. 2c and 2d, respectively.

[0020] At 12, a key is generated using, for example, processor 104 executing commands stored in memory 108 and is then stored in volatile memory 106, for example, Random Access Memory (RAM) of the processor 104. Encoding data using, for example, a cipher or encryption key and generation of the same is well known in the art and there are numerous encryption processes applicable. Depending on: the processing capability available; the digital data to be encoded; and, the security level to be ensured, one of skill in the art will readily select a suitable encryption process such as, for example, one of the symmetric encryption processes - Twofish, Serpent, AES, Blowfish, CAST5, RC4, TDES, and IDEA - to name a few. Alternatively, the key is generated outside the system 100, for example, using a trusted entity 125 installed in the server 124 or a key service provider connected to the server, transmitted to the device 120, 122 and received at port 102. Upon receipt, the key is then stored in the volatile memory 106.

[0021] At 14, digital data are received for storage, for example in a queue in the non-volatile memory 110. The received digital data are, for example, temporary digital data such as cache data or buffer data and are, for example, allocated to a temporary file directory. For example, temporary digital data are stored in non-volatile memory in the printer - received digital data for printing multiple copies; in the copier - digital data generated by scanning a document for printing multiple copies; in the fax machine - received digital data or digital data generated by scanning a document for sending multiple faxes; and in the workstation - temporary files of various applications for document recovery and temporary internet files for multiple access of a same website, to name but a few non-limiting examples. Upon receipt, using the processor 104, the digital data are encoded using the key stored in the volatile memory 106 - at 16 - in order to secure the same. The encoded digital data are then stored in the non-volatile memory 110 - at 18.

[0022] As long as there has been no interruption of supply of power - at 20 - to the volatile memory 106, the key is available enabling decoding the encoded digital data. For example, upon receipt of a request the processor 104 retrieves the encoded digital data from the non-volatile memory 110 - at 22 - decodes the retrieved encoded digital data using the key stored in the volatile memory 106 - at 24 - and provides the decoded digital data - at 26, for example, for printing multiple copies.

[0023] Upon interruption of supply of power to the volatile memory 106 - at 20 – data within the volatile memory 106 - i.e. the key - is erased - at 28. Absent the key, access to the encoded digital data stored in the non-volatile memory 110 is prevented. For example, the volatile memory 106 is erased upon power-down of the device 120, 122, 130. This provides a simple solution for securing temporary data stored in non-volatile memory without user intervention, i.e. when the device 120, 122, 130 is powered-down, for example, after office hours or for maintenance, access to the digital data stored in the non-volatile memory is automatically prevented. Accordingly, removing the non-volatile memory from the device 120, 122, 130 and retrieving the encoded digital data is futile. As is evident, techniques for detecting residual elements of a magnetic pattern remaining on the disk are also not useful in accessing the digital data for the same reason.

[0024] Optionally, the processor 104 also interrupts the power supply to the volatile memory 106 prior to switching of the device 120, 122, 130 into one of a stand-by mode and hibernation mode. Erasing the key prior to switching into the one of a stand-by mode and hibernation mode is beneficial in situations where the device 120, 122, 130 is used by numerous users, for example, a central copier in an office. For example, a dishonest employee is then prevented from printing documents belonging to colleagues at times, for example during lunch break, when the copier is not used but still powered-on.

[0025] Referring to Fig. 1b, shown is a simplified flow diagram of a method for securing data stored in non-volatile memory, according to an embodiment of the instant invention. As above, the method is described in connection with system 100, shown in Figs. 2a and 2b, for its implementation. Alternatively, the method is implemented using one of systems 200 and 300 of Figs. 2c and 2d, respectively. For the sake of clarity, same reference numerals are used for same method steps disclosed above.

[0026] During a first time period the method for securing data stored in non-volatile memory that is shown in Figure 1b is the same as described above for Figure 1a - steps 10 to 18 and steps 22 to 26 - securing temporary data by encoding the same using a first key. After elapse of a predetermined time interval a second key is generated - at 30. The first key stored in the volatile memory 106 is then replaced - at 32 - with the second key such that the first key is erased for preventing access to the digital data encoded using the first key, for example, by storing the

second key at the storage location of the first key in the volatile memory 106. For example the predetermined time interval relates to a period of time wherein no temporary data is queued within the device.

[0027] At 34, second digital data are received for storage in the non-volatile memory 110. Upon receipt, using the processor 104, the second digital data are encoded using the second key stored in the volatile memory 106 - at 36. The encoded second digital data are then stored in the non-volatile memory 110 - at 38. As long as there has been no interruption of supply of power - at 20 - to the volatile memory 106, the second key is available enabling decoding of the encoded digital data. For example, upon receipt of a request the processor 104 retrieves the encoded second digital data from the non-volatile memory 110 - at 40 - decodes the retrieved encoded second digital data using the second key stored in the volatile memory 106 - at 42 - and provides the decoded digital data - at 44, for example, for printing multiple copies.

[0028] Upon interruption of supply of power to the volatile memory 106 - at 20 – data within the volatile memory 106 - i.e. the key - is erased - at 28. Absent the key, access to the encoded second digital data stored in the non-volatile memory 110 is prevented. For example, the volatile memory 106 is erased upon power-down of the device 120, 122, 130.

[0029] Of course, it is possible to repeat the steps 30 to 44 numerous times, i.e. generating a new key after either a further predetermined time interval has elapsed or a predetermined event has occurred, and using the new key for encoding the received digital data, until the device 120, 122, 130 is powered-down.

[0030] For example, a new key is generated after predetermined time intervals; after completion of an application executed on the device - for example, after a web browser application is closed, access to the temporary internet files stored during this session is prevented by generating a new key; during a logoff process; and during a process for switching the device into one of a stand-by mode and hibernation mode. Alternatively, a new key is generated in dependence upon a state of the temporary data store and the future usefulness of data therein for its intended purpose. For example, an empty print queue prompts generation of a new key.

[0031] The above methods for securing data stored in non-volatile memory are implementable using the system 100 shown in Figs. 2a and 2b. As shown in Figs. 2a and 2b, the system 100

comprises the processor 104 connected to the communication and output port 102, for example, a Universal Serial Bus (USB) port or an Advanced Technology Attachment (ATA) port such as an Integrated Drive Electronics (IDE) port, the volatile memory 106, for example, RAM of the processor 104, the memory 108, and the non-volatile memory 110. The processor 104 generates or receives the key; stores the key in the volatile memory 106; encodes the received digital data using the key and stores the encoded digital data in the non-volatile memory 110; retrieves the encoded digital data and decodes the retrieved encoded digital data using the key stored in the volatile memory 106. The processor 104 performs the method by executing executable commands stored in the memory 108. Alternatively, the processor 104 comprises electronic circuitry designed for performing the method in a hardware implemented fashion, thus allowing omission of the memory 108. Optionally, the method for securing data stored in non-volatile memory is implemented using the processor and volatile memory of the device by providing executable commands stored in a storage medium for execution on the processor, for example, for implementation on a workstation.

[0032] Alternatively, in the system 200 that is shown in Fig. 2c the processor 104, the volatile memory 106, and the memory 108 are disposed, for example, on a Printed Circuit Board (PCB) which is inserted into an expansion slot of the device, for example, a workstation, and connected to the non-volatile memory 110 of the device via bus system 212 connected to the communication and output port 102, for example, a Universal Serial Bus (USB) port or an Advanced Technology Attachment (ATA) port such as an Integrated Drive Electronics (IDE) port. Optionally, the processor 104 comprises electronic circuitry designed for performing the method in a hardware-implemented fashion, and RAM of the processor is used for storing the key. This enables implementation of the above method for securing data stored in non-volatile memory by providing a single chip, for example, a Field Programmable Gate Array (FPGA) for insertion into an appropriate socket of the device.

[0033] Further alternatively, as shown in the system 300 according to the invention of Fig. 2d, the processor 104, the volatile memory 106, the memory 108, and the non-volatile memory 110 are disposed within a single housing 301 and are connected to, for example, a bus system of the device via the communication and output port 102, for example, a Universal Serial Bus (USB) port or an Advanced Technology Attachment (ATA) port such as an Integrated Drive Electronics

(IDE) port. Optionally, the processor 104 comprises electronic circuitry designed for performing the method in a hardware-implemented fashion, and RAM of the processor is used for storing the key.

[0034] As is evident, the systems shown in Figs. 2a to 2d are implementable as a retrofit in existing devices, for example, by providing executable commands for execution on a processor of a workstation - system 100, by inserting a PCB into an insertion slot of a workstation - system 200, and by replacing the hard drive of a copier with the system 300.

[0035] Numerous other embodiments of the invention will be apparent to persons skilled in the art without departing from the spirit and scope of the invention as defined in the appended claims.

CLAIMS

What is claimed is:

1. A method comprising:

providing a device comprising a non-volatile memory;

receiving digital data for being stored in the non-volatile memory;

prior to storing the digital data in the non-volatile memory, encoding the digital data using a key stored in a volatile memory that is supplied with power only when the device is in a powered-on condition, the volatile memory for being erased automatically upon interruption of supply of power thereto, the encoding for preventing access to the digital data in a non-encoded form absent the key;

storing the encoded digital data in the non-volatile memory; and,

subsequent to storing the encoded digital data in the non-volatile memory, erasing the key from the volatile memory.

2. A method according to claim 1, wherein erasing the key from the volatile memory is performed in response to one of the device entering a low-power mode, the device being powered-down, elapse of a predetermined time interval during which the device is inactive, and receipt of a command for erasing the key from the volatile memory.

3. A method as defined in claim 1 or 2, wherein receiving digital data comprises receiving temporary digital data.

4. A method as defined in claim 3, wherein receiving temporary digital data comprises receiving digital data for storing within the volatile memory pending encoding and storage in the non-volatile memory.

5. A method as defined in claim 3, wherein receiving temporary digital data comprises receiving temporary Internet files.

6. A method as defined in claim 3, wherein receiving temporary digital data comprises receiving temporary digital data allocated to a temporary file directory.

7. A method as defined in any one of claims 1 to 6, wherein providing a device comprises providing one of a computer, a printer, a copier, a scanner, a projection display, and a fax machine.

8. A method as defined in any one of claims 1 to 7, wherein the volatile memory is erased upon power-down of the device.

9. A method as defined in any one of claims 1 to 8, comprising:
retrieving the encoded digital data from the non-volatile memory;
decoding the retrieved encoded digital data using the key stored in the volatile memory; and,
providing the decoded digital data.

10. A method as defined in any one of claims 1 to 9, comprising:
generating the key; and,
storing the key in the volatile memory.

11. A method as defined in claim 10, wherein the key is generated using a processor of the device.

12. A method as defined in claim 10, wherein the key is generated using a processor other than a processor of the device and wherein the key is provided to the device subsequent to being generated.

13. A method as defined in claim 10, comprising:
generating a second key; and,
replacing the key stored in the volatile memory with the second key.

14. A method as defined in claim 13, wherein the key is replaced with the second key such that the key is erased.

15. A method as defined in claim 13, wherein the second key is generated after elapse of a predetermined time interval wherein a queue having the encoded data stored therein is empty.

16. A method as defined in claim 13, wherein the second key is generated after elapse of a predetermined time interval.

17. A method as defined in claim 13, wherein the second key is generated after completion of at least one of an application executed on the device and a process completed by the device.

18. A method as defined in claim 13, wherein the second key is generated during a process for switching the device into one of a stand by mode and a hibernation mode.

19. A method as defined in claim 13, wherein the second key is generated during a logoff process.

20. A system comprising:
volatile memory for storing a key therein, the volatile memory for being erased upon interruption of supply of power thereto;
a communication and output port;
circuitry connected to the communication and output port, to the volatile memory and for being connected to non-volatile memory of a device, the circuitry for:

receiving temporary digital data for storage in the non-volatile memory of the device;
encoding the temporary digital data using the key stored in the volatile memory, the encoding for preventing access to the encoded temporary digital data absent the key, the key other than stored within non-volatile memory of the device;
providing the encoded temporary digital data for storage in the non-volatile memory;
retrieving the encoded temporary digital data from the non-volatile memory;
decoding the retrieved encoded temporary digital data using the key stored in the volatile memory; and,
providing the temporary digital data.

21. A system as defined in claim 20, comprising second circuitry connected to the volatile memory, the second circuitry for generating the key.

22. A system as defined in claim 20 or 21, wherein the communication and output port comprise one of a universal serial bus port and an advanced technology attachment port.

23. A system as defined in any one of claims 20 to 22, comprising non-volatile memory for storing temporary digital data therein.

24. A computer readable storage medium having stored thereon executable commands for execution on a processor, the processor when executing the commands performing:
one of generating a key and receiving a key for use in encoding;
storing the key in volatile memory;
receiving digital data for storage in non-volatile memory of a device;
encoding the digital data using the key stored in the volatile memory, the encoding for preventing access to the encoded digital data in a non-encoded form absent the key, the key other than stored within non-volatile memory of the device;
providing the encoded digital data for storage in the non-volatile memory;
retrieving the encoded digital data from the non-volatile memory;
decoding the retrieved encoded digital data using the key stored in the volatile memory; and,
providing the digital data.

25. A computer readable storage medium as defined in claim 24, wherein the processor when executing the commands performs receiving temporary digital data.

26. A method comprising:
providing a device for processing digital data and comprising a queue, the queue comprising non-volatile memory;
receiving digital data for being stored within the queue and processed by the device;
ciphering the received digital data with a key to provide secure data, the key stored in volatile memory and for being erased when at least one of power is other than provided to the volatile memory and the received digital data has been ciphered;

storing the secure data within the queue;

retrieving the secure data from the queue;

deciphering the secure data using the key stored in volatile memory; and

processing the deciphered secure data.

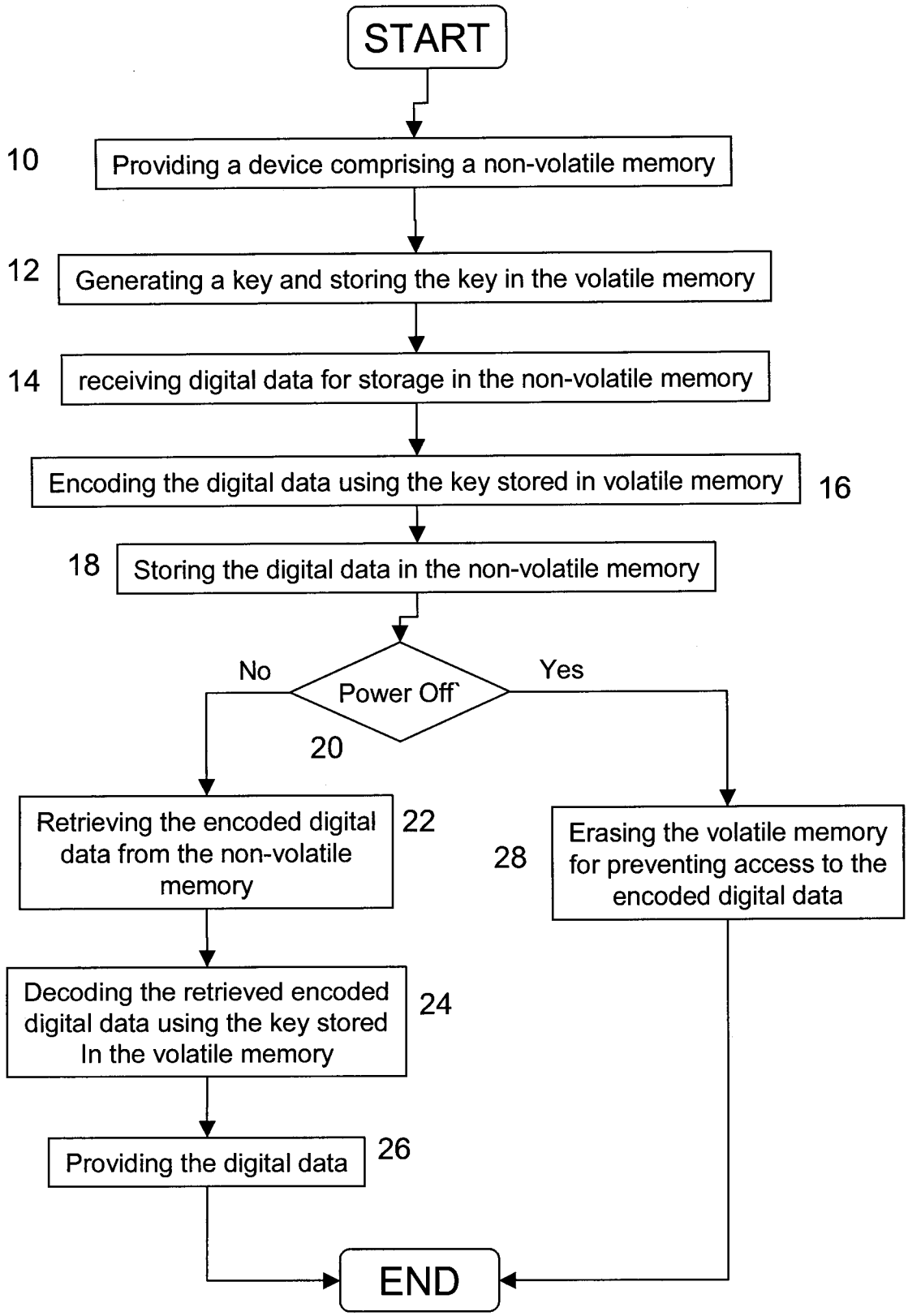
START
10
Providing a device comprising a non-volatile memory
12
Generating a key and storing the key in the volatile memory
14
receiving digital data for storage in the non-volatile memory
Encoding the digital data using the key stored in volatile memory
16
18
Storing the digital data in the non-volatile memory
No
Power Off
Yes
20
Retrieving the encoded digital data from the non-volatile memory
22
28
Erasing the volatile memory for preventing access to the encoded digital data
Decoding the retrieved encoded digital data using the key stored In the volatile memory
24
Providing the digital data
26
END

Fig. 1A

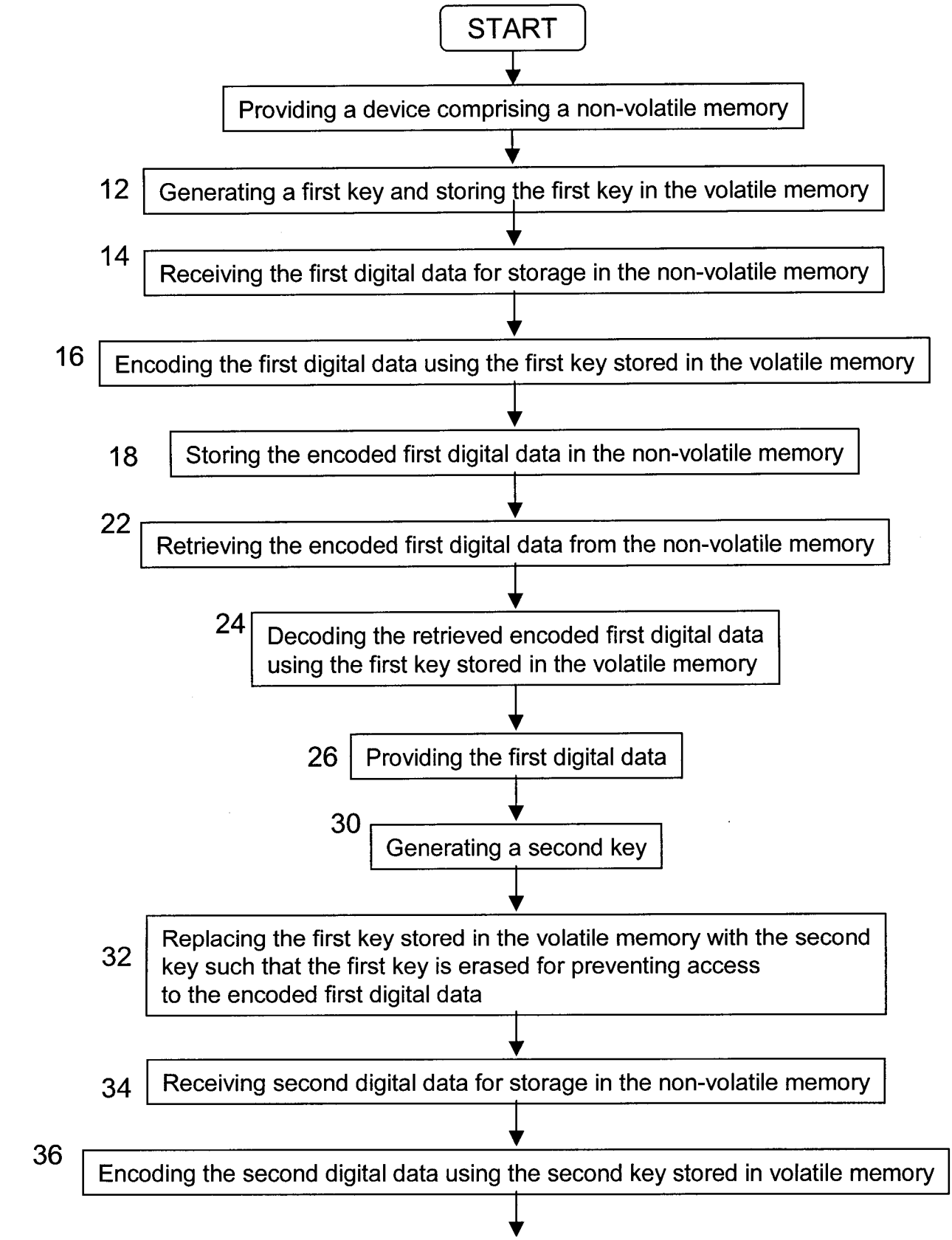
START
Providing a device comprising a non-volatile memory
12
Generating a first key and storing the first key in the volatile memory
14
Receiving the first digital data for storage in the non-volatile memory
16
Encoding the first digital data using the first key stored in the volatile memory
18
Storing the encoded first digital data in the non-volatile memory
22
Retrieving the encoded first digital data from the non-volatile memory
24
Decoding the retrieved encoded first digital data using the first key stored in the volatile memory
26
Providing the first digital data
30
Generating a second key
32
Replacing the first key stored in the volatile memory with the second key such that the first key is erased for preventing access to the encoded first digital data
34
Receiving second digital data for storage in the non-volatile memory
36
Encoding the second digital data using the second key stored in volatile memory

Fig. 1B

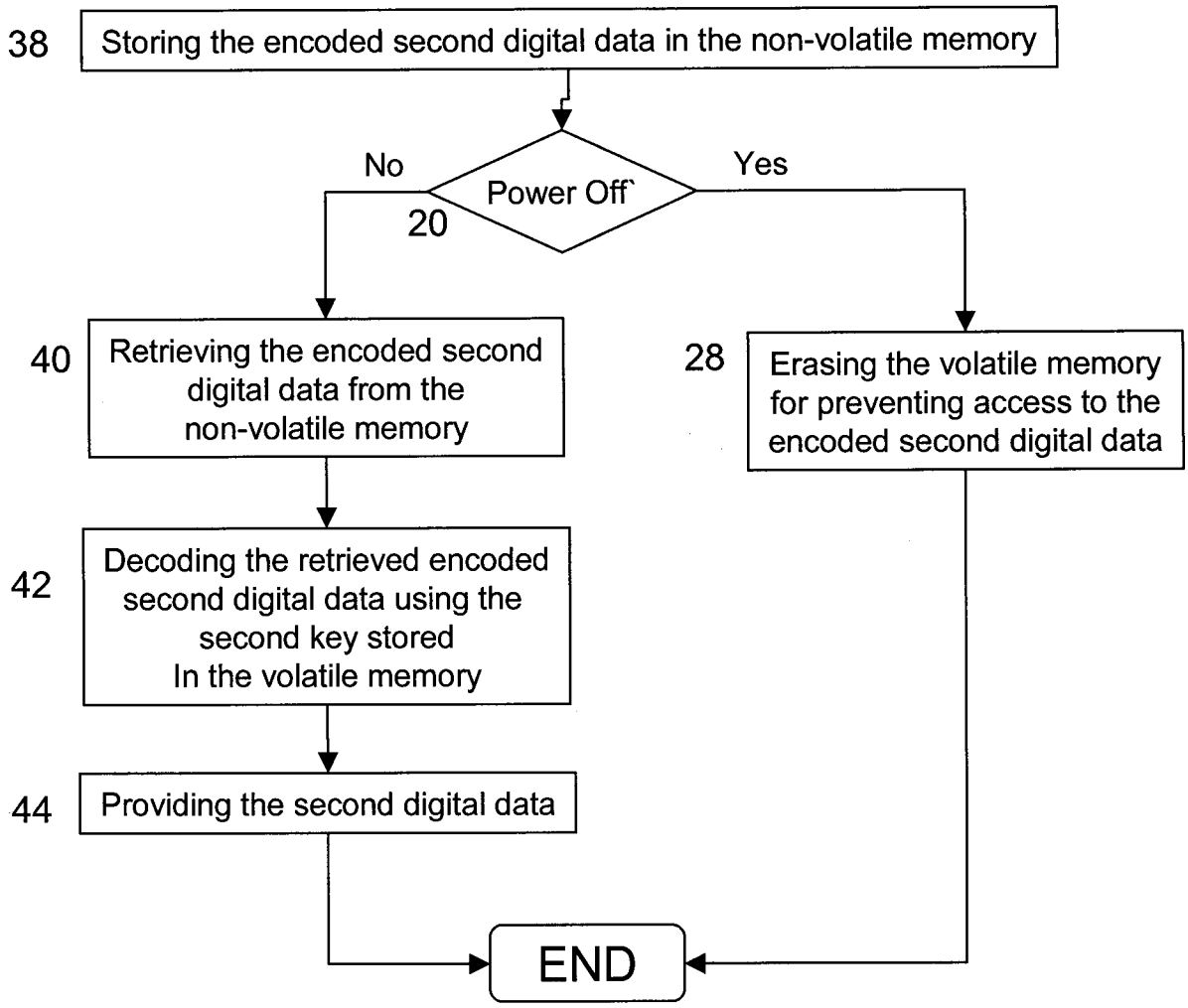

Fig. 1B (Continued)

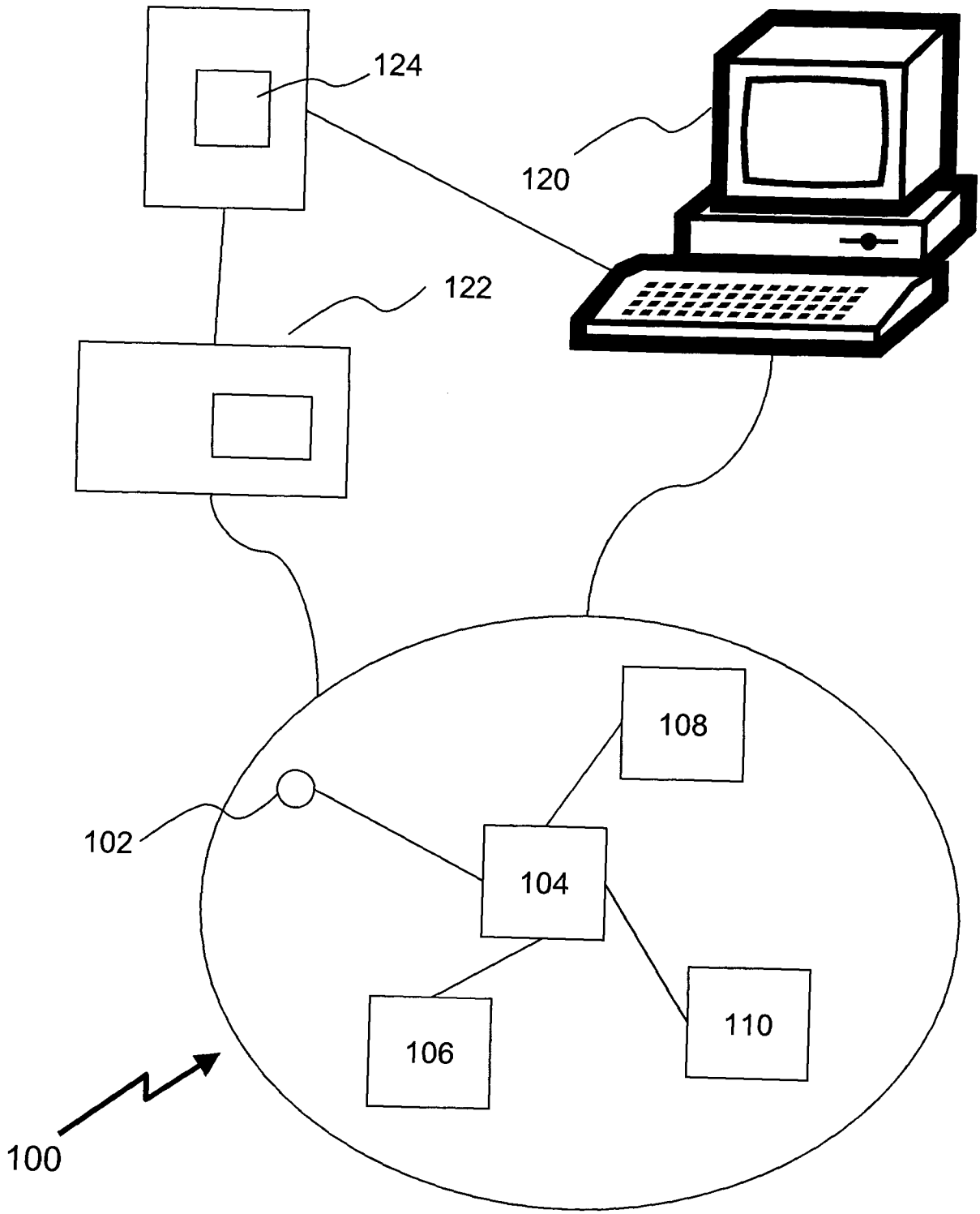

Fig. 2A

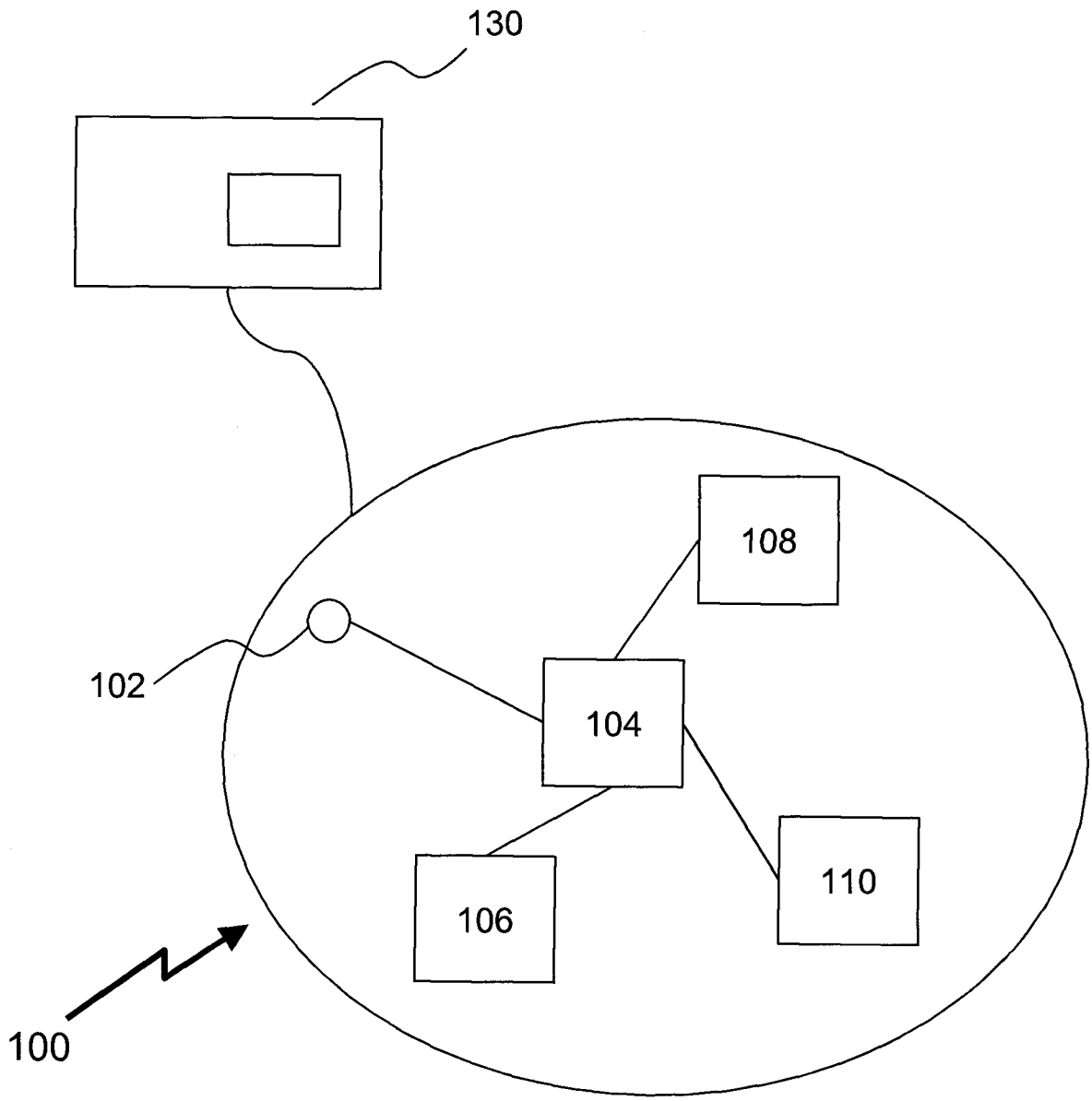

Fig. 2B

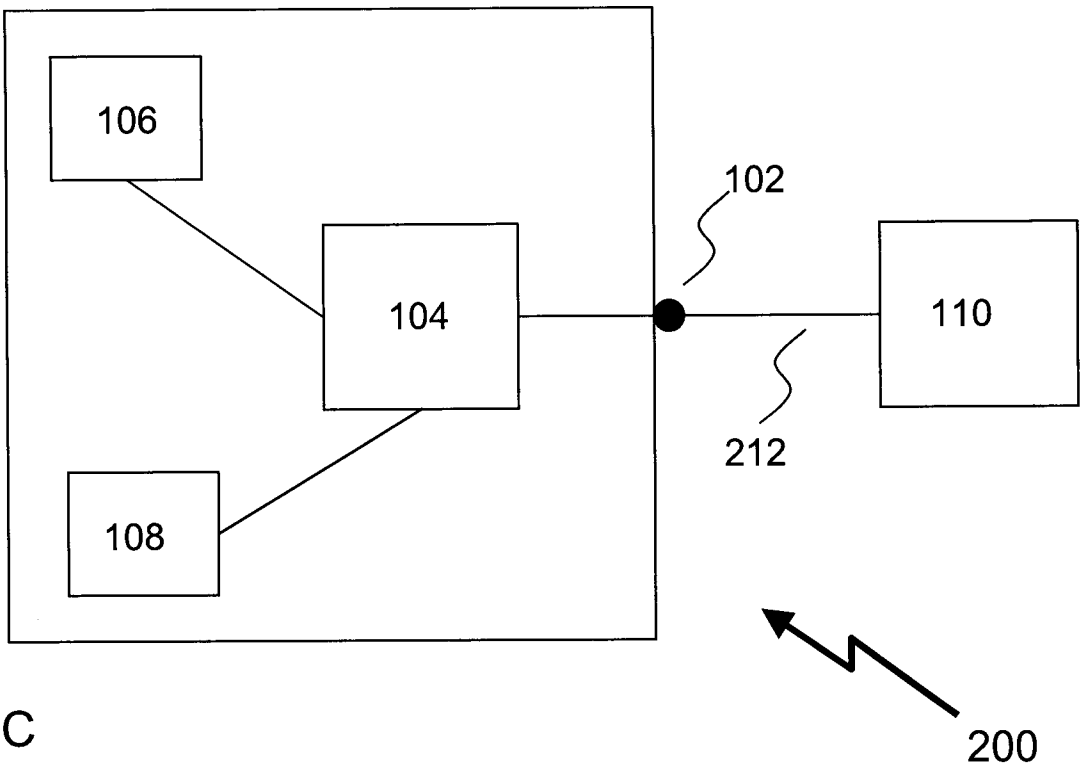

Fig. 2C

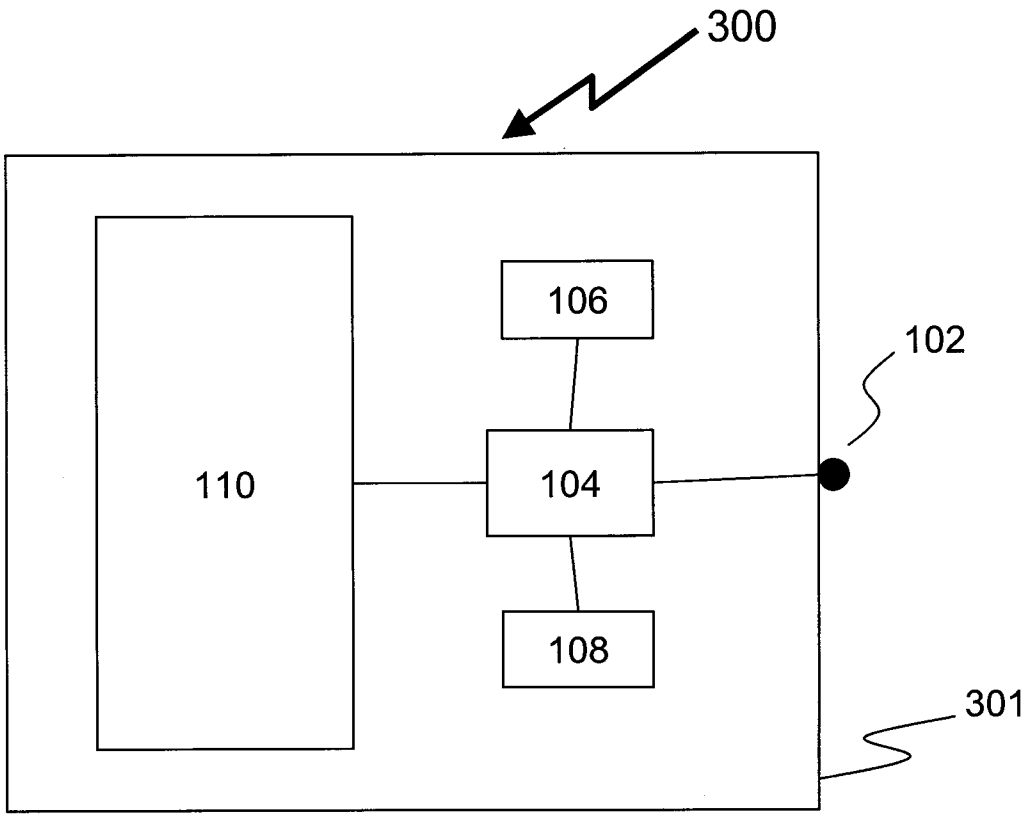

Fig. 2D

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2008/001218

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06F 21/24*** (2006.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F (2006.01)

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Databases: Canadian Patents Database, WEST, Delphion, Google Patents, IEEE XPLORE
Keywords: secur*, encrypt*, decrypt*, key, volatile, non-volatile, RAM, power-off, power-down, eras*, delet*, inactiv*,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 5,677,952 (Blakley et al.) 14 October 1997 (14-10-1997) * Fig. 2; col. 4, lines 22 - 25; col. 5, lines 31 - 40; col. 6, lines 25 - 57 *	1 - 11, 20, 24 - 26 12 - 19, 21 - 23
Y	US 5,412,721 (Rager et al.) 2 May 1995 (02-05-1995) * Fig. 1; col. 5, lines 22 - 61 *	1 - 26
Y	US 2007/0101158 A1 (Elliott) 3 May 2007 (03-05-2007) * Fig. 1, refs 100, 114, 112, 102; par. [0009] - [0024] *	1 - 26
Y	US 6,928,551 B1 (Lee et al.) 9 August 2005 (09-08-2005) * Abstract; col. 5, line 48 - col. 7, line 4 *	1 - 26
Y	US 5,249,227 (Bergum et al.) 28 September 1993 (28-09-1993) * col. 1, line 58 - col. 3, line 59 *	1 - 26
Y	US 5,457,748 (Bergum et al.) 10 October 1995 (10-10-1995) * Abstract; col. 1, line 56 - col. 4, line 39 *	1 - 26

[X] Further documents are listed in the continuation of Box C. [X] 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 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	Date of mailing of the international search report
30 October 2008 (30.10.2008)	5 November 2008 (05-11-2008)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Raghid Shreih 819- 994-2694

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2008/001218

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 2006/0020823 A1 (Morino) 26 January 2006 (26-01-2006) * Whole Document *	
A	US 3,956,615 (Anderson et al.) 11 May 1976 (11-05-1976) * Whole Document *	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2008/001218

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US 5677952A	14-10-1997	DE 69431390D1	24-10-2002
		DE 69431390T2	05-06-2003
		EP 0658022A2	14-06-1995
		EP 0658022A3	14-06-2000
		EP 0658022B1	18-09-2002
		JP 3320928B2	03-09-2002
		JP 7199808A	04-08-1995
		SG 44363A1	19-12-1997
		US 5454039A	26-09-1995
		US 5675652A	07-10-1997
		US 5835597A	10-11-1998
US 5412721A	02-05-1995	AU 662685B2	07-09-1995
		AU 6442594A	24-10-1994
		CA 2135631A1	13-10-1994
		CA 2135631C	26-01-1999
		GB 2282036A	22-03-1995
		GB 2282036B	05-02-1997
		GB 9422583D0	04-01-1995
		WO 9423512A1	13-10-1994
US 2007101158A1	03-05-2007	None	
US 6928551B1	09-08-2005	None	
US 5249227A	28-09-1993	CA 2127539A1	09-06-1994
		CA 2127539C	29-12-1998
		EP 0627142A1	07-12-1994
		EP 0627142A4	12-07-2000
		JP 2727763B2	18-03-1998
		JP 7503595T	13-04-1995
		WO 9413079A1	09-06-1994
US 5457748A	10-10-1995	DE 69332543D1	16-01-2003
		DE 69332543T2	24-04-2003
		EP 0671090A1	13-09-1995
		EP 0671090A4	12-07-2000
		EP 0671090B1	04-12-2002
		JP 8504067T	30-04-1996
		WO 9413080A1	09-06-1994
US 2006020823A1	26-01-2006	None	
US 3956615A	11-05-1976	CA 1059630A1	31-07-1979
		DE 2527784A1	15-01-1976
		DE 2527784C2	30-08-1984
		FR 2276639A1	23-01-1976
		FR 2276639B1	09-12-1977
		GB 1458495A	15-12-1976
		IT 1039308B	10-12-1979
		JP 1142598C	13-04-1983
		JP 51006632A	20-01-1976
		JP 57035499B	29-07-1982