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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/41357 A1

(51) International Patent Classification[7]: H04L 9/28

(21) International Application Number: PCT/US00/30164

(22) International Filing Date:
28 November 2000 (28.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/453,291 3 December 1999 (03.12.1999) US

(71) Applicant *(for all designated States except US)*: **CIPHERACTIVE COMMUNICATION SECURITY LTD.** [IL/IL]; P.O. Box 2202, 39120 Tirat Hacarmel (IL).

(71) Applicant *(for TJ only)*: **FRIEDMAN, Mark, M.** [US/IL]; 1 Alharizi Street, 43406 Raanana (IL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **BRANDMAN, Nahum** [IL/IL]; 11/32 Biram Street, 34986 Haifa (IL).

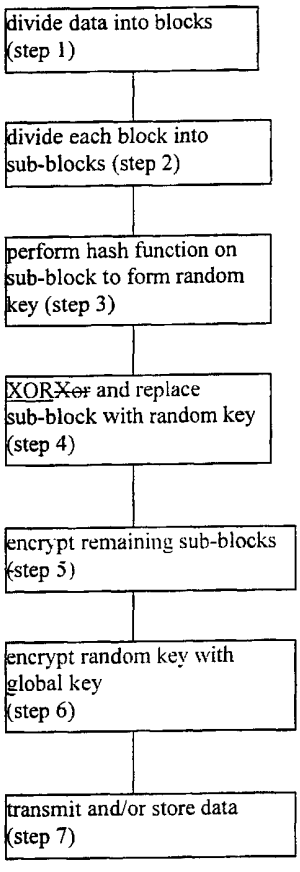
(74) Common Representative: **FRIEDMAN, Mark, M.**; c/o Castorina, Anthony, Suite 207, 2001 Jefferson Davis Highway, Arlington, VA 22202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: ENCRYPTION OF PARTITIONED DATA BLOCKS UTILIZING PUBLIC KEY METHODS AND RANDOM NUMBERS



(57) Abstract: Referring to the figure, a system and a method for more rapidly and efficiently encrypting data with a global key, by scrambling a first portion of the data according to a non-reversible function such as a hash function (step 3) and then encrypting the scrambled data with the random generated key (step 5), preferably according to a weaker and faster encryption method. The remaining data, which contains the local data key can then optionally be encrypted with a stronger encryption method (step 6). Preferably, the first portion of data is a relatively larger fraction of the overall data, for increased efficiency of encryption. However, the system and method effectively provide the highest level of data security overall, at the level provided by the strong encryption method, even though only a portion of the data is encrypted according to the strong encryption method. Thus, the system and method are both more efficient and more effective than the background art encryption methods.

WO 01/41357 A1

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

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.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ENCRYPTION OF PARTITIONED DATA BLOCKS UTILIZING PUBLIC KEY METHODS AND RANDOM NUMBERS

FIELD AND BACKGROUND OF THE INVENTION

The present invention relates to a system and method for video, audio and data encryption, and in particular to such a system and method in which the efficiency of encryption is increased by encrypting a first portion of the data according to a strong encryption protocol and a second portion of the data according to a rapid encryption protocol, such that effectively the entirety of the data cannot be accessed without the key for the strong encryption protocol.

As increasing amounts of data are transmitted through the Internet and other networks, the need has grown for strong and efficient encryption methods in order to protect the transmitted data. Since the Internet is not truly peer-to-peer, transmitted data can unfortunately be accessed relatively easily by unauthorized users. For example, the transfer of sensitive financial data, confidential business information and the electronic transfer of proprietary information of commercial institutions, must remain confidential and protected. Other examples of sensitive data include securities information related to the stocks and securities community, medical information for patients, stored and retrieved business data and so forth.

Although a number of encryption methods are currently available for protecting data for transmission, all of these encryption methods suffer from disadvantages. Strong methods of encryption require extensive computing resources and time for performance. Weaker encryption methods are easy to overcome, such that the encrypted data is still vulnerable to access by unauthorized personnel. Thus, clearly new methods for encrypting data are required in order to efficiently encrypt data for transmission and in order to effectively protect the data during transmission and/or storage.

For example, the Data Encryption Standard (DES) could be used with a commonly generated global key, where the global key is generated using public key cryptographic techniques. The 3DES implementation in software

programs is inefficient because of the complicated, computationally intensive algorithm, which requires a powerful processor as well as large amount of time to perform calculations for each block of data. For wide bandwidth data, such as video stream data, the time and processor requirement is undesirable and economically unjustified.

PCT Application No. WO 99/44364 discloses an improved encryption method, in which the data to be encrypted is first divided into blocks. Certain blocks are scrambled according to a one-to-one function with other blocks, which are not scrambled. These blocks are then encrypted with the global key. The combination of scrambling the data with the encryption prevents the data from being understood by an unauthorized user. However, the one-to-one function has the disadvantage of being reversible, such that the original data can be regenerated from the scrambled data by performing the reverse of the function. Furthermore, such one-to-one functions are more vulnerable to being "cracked" by unauthorized users, even without access to the particular function itself and/or the key which was used to scramble the data.

A more secure method would not use a one-to-one function for scrambling the scrambled blocks of data, but instead would use a function which is not reversible. Such a method could also incorporate different types of encryption for various portions of the data, since the scrambled data itself would be significantly less accessible to the unauthorized user. Unfortunately, such a secure method is not currently available.

There is thus a need for, and it would be useful to have, a system and a method for encrypting data in which the data is divided into blocks and sub-blocks, some of which are scrambled according to a non-reversible function, such that different portions of the data can be encrypted according to encryption methods of different strengths for more efficient encryption of the data, while still maintaining the overall strength of the protection of the data at the high level of the strongest encryption method.

SUMMARY OF THE INVENTION

The present invention is of a system and a method for more rapidly and efficiently encrypting data with a global key, by scrambling a first portion of the data according to a non-reversible function such as a hash function and then optionally, encrypting the scrambled data with the generated random local-data key, which is defined as a XOR combination of the hash function and the second portion of the data. The encryption method, which is used to encrypt the first portion of the data could optionally and preferably be weak but rapidly performed. Preferably, the first portion of data is a relatively large fraction of the overall data, for increased efficiency of encryption.

The second part of the data, which is preferably the smaller portion of the data, contains the local-data key "XOR"-ed with the smallest second portion. This second part of the data is optionally and preferably encrypted using a Public key, defined as a Global Key, more preferably with a stronger encryption method of any kind.

The system and method of the present invention effectively provide the highest level of data security overall, at the level provided by the strong encryption method, even though only a portion of the data is encrypted according to the strong encryption method. As used herein, the terms "stronger encryption method" and "weaker encryption method" are relative, such that the results of the stronger encryption method are more difficult to break than the results of the weaker encryption method. Thus, the system and method of the present invention are both more efficient and more effective than background art encryption methods.

According to the present invention, method for encrypting data with a global key is provided, the data being divided into a plurality of blocks, the steps of the method being performed by a data processor, the method comprising the steps of: (a) dividing each block into at least two sub-blocks, denoted as a first sub-block and a second sub-block; (b) combining said first sub-block with said second sub-block with a hash function to form a scrambled sub-block of data as a random key; (c) replacing said second sub-block with

said random key; (d) encrypting said first sub-block of data; and (e) encrypting said random key with the global key.

According to another embodiment of the present invention, a system is provided for encrypting data with a global key, the data being divided into a plurality of blocks, the system comprising: (a) a data input device for receiving the blocks of data; (b) a sub-block division module for dividing the blocks of data into sub-blocks; (c) a scrambling module for performing a non-reversible function on at least one sub-block of data to form scrambled data; (d) a random key module for replacing the at least one sub-block with the scrambled data and for encrypting the scrambled data with the random local- data key; and (e) a remainder encryption module for encrypting the random local-data key with a global key.

Hereinafter, the term "computer platform" refers to a particular computer hardware system or to a particular software operating system. Examples of such hardware systems include, but are not limited to, personal computers (PC), palmtop computers, handheld and portable computers, Macintosh ™ computers, mainframes, minicomputers, various types of data processors including ASIC, DSP, and RISC processors, workstations. Examples of such software operating systems include, but are not limited to, UNIX, VMS, Linux, MacOS™, DOS, one of the Windows™ operating systems by Microsoft Corp. (USA), including Windows NT™, Windows 3.x™ (in which "x" is a version number, such as "Windows 3.1™"), Windows CE™, Windows95™, and Windows98™, as well as any suitable operating system for embedded units or palmtop/handheld type portable computers.

For the present invention, a software application could be written in substantially any suitable programming language, which could easily be selected by one of ordinary skill in the art. The programming language chosen should be compatible with the computer platform according to which the software application is executed. Examples of suitable programming languages include, but are not limited to, C, C++ and Java.

In addition, the present invention could be implemented as software, firmware or hardware, or as a combination thereof. For any of these implementations, the functional steps performed by the method could be described as a plurality of instructions performed by a data processor.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

FIG. 1 is a flowchart of an exemplary method for encrypting data according to the present invention;

FIG. 2 is a schematic block diagram for describing a preferred embodiment of the method of Figure 1; and

FIG. 3 is a schematic block diagram of an exemplary system according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is of a system and a method for more rapidly and efficiently encrypting data with a global key, by scrambling a first portion of the data according to a non-reversible function such as a hash function, and then replacing the local data key with the second portion of data. The scrambled, first portion of data is then encrypted with the local-data key. Next, the second portion of the data is replaced with a global key, preferably according to a strong encryption method. The first portion of data may then optionally be encrypted with a weak encryption method. Preferably, the first portion of data is a relatively large fraction of the overall data, for increased efficiency of encryption. However, the system and method of the present invention effectively provide the highest level of data security overall, at the level provided by the strong encryption method, even though only a portion of the data is encrypted according to the strong encryption method. Thus, the system and method of the present invention are both more efficient and more effective than background art encryption methods.

Examples of background art encryption methods which may be employed with the present invention also include, but are not limited to, Diffie-Hellman, as disclosed in U.S. Patent No. 4,200,770; RSA, as disclosed in U.S. Patent No. 4,405,829; and Hellman-Pohlig, as disclosed in U.S. Patent No. 4,424,414; all of which are hereby incorporated by reference as if fully set forth herein.

The principles and operation of the system and method according to the present invention may be better understood with reference to the drawings and the accompanying description.

Referring now to the drawings, Figure 1 shows a flowchart of an exemplary method for encrypting data according to the present invention. As described in greater detail below with regard to Figure 3, various types of data can optionally be encrypted according to the method of the present invention. The exemplary method assumes that a global key is publicly available for a public-key encryption method, which is highly preferred for the operation of the present invention. However, it is understood that other types of encryption methods and key generating schemes, such as ECC (elliptic curve cryptography), could also be used with the method of the present invention.

In step 1 of Figure 1, the data is divided into a plurality of blocks. The size of the blocks is dependent upon the type of data and/or upon the type of encryption to be performed at subsequent steps. However, a typical preferred block size is 512 bits. In step 2, each block is divided into at least two sub-blocks, denoted as a first sub-block and a second sub-block, although optionally the data may be divided into a larger number of sub-blocks, as described in greater detail below with regard to Figure 2. Preferably, each sub-block is 64 bits in size if the DES group of encryption methods is used to encrypt the data.

In step 3, a hash function is performed to combine the first sub-block of data with the second sub-block of data, for example with an XOR (exclusive "or") function. The performance of the hash function results in a scrambled sub-block of data, which then forms a random key. The random key is thus

data dependent, and as such cannot be predicted by analyzing previous sub-blocks of data and/or by analyzing previous blocks of data. Indeed, a change to a single bit of the block of data would change the random key. Thus, unless the unauthorized user had access to all of the data, the random key could not be obtained by analytical methods of "cracking" the ciphertext.

Optionally, an extension to the performance of the hash function would involve the operation of the MD5 algorithm or any other one-way hash function including but not limited to those functions which are described in "Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C", Bruce Schneier, ISBN 0-471-12845-7, Katherine Schowalter, John Wiley & Sons, Inc.

In step 4, the second sub-block is replaced with the random key. In step 5, the first sub-block of data is encrypted, optionally and preferably with a weaker but more rapidly performed method of encryption, such as the original DES encryption method for example.

In step 6, the random key is encrypted with the global key, preferably with a strong encryption method such as the 3DES encryption method for example. The term strong encryption method refers generally to the level of security of the encryption algorithm, such that a strong encryption method provides a higher level of security. For example, it generally believed that the 3DES encryption method is stronger than the DES encryption method. Another example of a strong encryption method is IDEA. By contrast, a weak encryption method provides a lower level of security. In step 7, the encrypted data may now be transmitted and/or stored, for example. Various options for using the encrypted data are described in greater detail with regard to Figure 3.

One advantage of the method of the present invention is that real-time encryption is significantly accelerated, since a high overall level of security can be provided for the entirety of the data, even if only a small portion of the data is encrypted with the strong encryption method, while the remainder of the data is encrypted with a weaker but more efficient encryption method. Therefore, the rate of encryption is significantly accelerated, which is particularly

important for real-time and other highly time-sensitive encryption applications. For such applications, any delay is unacceptable. Thus, the method of the present invention provides strong encryption security for a fraction of the computational time and processing requirements.

Another advantage of the method of the present invention is that the RC4 encryption method, or any fast stream cipher method in which data must be encrypted as a stream rather than as discrete units, can be used to encrypt the data. The RC4 encryption method is a strong and efficient method of encryption, but has the disadvantage of being unsuitable for data, which is organized into packets or other discrete units. This disadvantage arises from the requirement of the algorithm for a random key in order to encrypt the data, as the strength of this particular encryption algorithm lies with the use of the random key. Previous applications of the RC4 algorithm would therefore result in the same random key being used for encrypting all of the packets in a particular transmission, which would render the encrypted data highly vulnerable to being "cracked" or decrypted from ciphertext back to plaintext by an unauthorized user. The method of the present invention overcomes this disadvantage by providing a random key, which is generated separately for each unit of data such as a packet. Thus, the method of the present invention could use the RC4 algorithm for encrypting the second sub-block of data, for example.

Another advantage of the method of the present invention is that the method permits a combination of a block cipher with a stream cipher. Yet another advantage of the method of the present invention is that the method could be divided into two or more stages to provide protection for data which is to be stored, as well as for data which is to be retrieved, broadcast and/or browsed one or more times, in real time and on-demand. The first stage would preferably be a "pre-encryption process". The method could perform the "pre-encryption process" as defined below during the process of storing digital files or compressed data, by using relatively few computational functions, which do not consume a significant portion of the time required for performing

the total process.

At least a portion of the method is preferably performed "off-line" or "near-line" for the post-compression of data before transmission or storage. This portion of the method preferably includes the step of first: Dividing each block into at least two sub-blocks, denoted as a first sub-block and a second sub-block. Next, the first sub-block is combined with the second sub-block with a hash function to form a scrambled sub-block of data as a random key. In step 3, the second sub-block is replaced with the random key.

The benefits of using this method include the following. First, the stored content is in a protected format. Second, the method does not encrypt the header or trailers of relevant packages, which are used for indexing functions, for example in order to browse through stored, encrypted data for retrieval of such data. Third, the method does not add one or more redundant bits to the data; unlike background art methods, which do add such bits.

Preferably, the second stage is performed upon demand for the retrieval, broadcast, remote transmission and/or browsing of the protected stored data. The second stage preferably includes the step of encrypting the random key with the global key.

The benefits of the second stage include the following. First, the protected stored data can be transmitted in a highly secure form to a remote storage location, since the highly secure encryption of the data is now added with the preferred strong encryption method. Second, if multiple subscribers request the same content, the method of the present invention would only require encryption of the designated sub-block containing the local data key with the subscriber public (Global) key, rather than encrypting the whole file or block. Therefore, such an encryption process clearly requires fewer computational resources to perform and is therefore more efficient.

Furthermore, for gateway and router key switching applications, the method would only require encryption of the designated sub-block containing the local data key with the subscriber public (Global) key, as compared to the process of encrypting the whole data package, which passes the unit.

According to another preferred embodiment of the present invention, steps 1-5 of the method of Figure 1 are performed in a pre-processing stage. This pre-processing stage is preferably performed off-line or near off-line for data storage purposes, including but not limited to, creating secure physical and virtual data storage volumes or "snap-shots" of stored data, or used for remote back-up and mirroring of data.

Figure 2 is a schematic block diagram of a preferred but exemplary implementation of the method of Figure 1. As noted previously, the block of data may be of substantially any size, and may be divided into substantially any number of a plurality of sub-blocks of substantially any size. For example, for a block of data of 512 bits, the plurality of sub-blocks may be 16 sub-blocks of 32 bits per sub-block, 8 sub-blocks of 64 bits per sub-block, 4 sub-blocks of 128 bits per sub-block, and so forth.

In the example of Figure 2, the block of 512 bits of data is divided into 8 sub-blocks of 64 bits per sub-block, designated as "d1" through "d8". The block of data also features a footer and header. Therefore, for the method of Figure 1 as performed on the data structure of Figure 2, sub-blocks d1 to d7 would be scrambled with sub-block d8 according to a hash function to form the random key. The random key would then replace sub-block d8. A fast cipher like RC4 or DES encryption method would optionally be used to encrypt sub-blocks d1 to d7, for example, with the global key. A high-level cipher 3DES encryption method would optionally be used to encrypt sub-block d8, for example.

Also as shown in Figure 2, another advantage of the method of the present invention is that a plurality of global keys could be used to encrypt the data without re-encrypting the entirety of the data with each global key. Instead, only the random key, which replaced sub-block d8 in this example, would need to be re-encrypted with each global key. The remaining sub-blocks would only need to be encrypted once, regardless of the number of different global keys, which are used. Thus, such an implementation is clearly more

efficient for encryption when multiple global keys are required, for example for a system with multiple users and/or subscribers.

Figure 3 is a schematic block diagram of an exemplary system according to the present invention. A system **10** features a data input device **12** for inputting data, which may be any type of broadcasting application. System **10** is also assumed to have received a global key. Data input device **12** is optionally connected to a sub-block division module **14** for dividing the data into blocks and sub-blocks, if the data is not already divided into blocks and/or sub-blocks.

A scrambling module **16** then receives the blocks and sub-blocks of data, and performs a non-reversible function, such as a hash function, on at least one sub-block of data to form scrambled data. A random key module **18** then replaces a designated sub-block with the scrambled data, to form an encrypted random key. A remainder encryption module **20** then encrypts the remainder of the sub-blocks for each block to form encrypted sub-blocks, preferably with a weaker but more rapidly performed encryption method as previously described. The encrypted sub-blocks and random key may then optionally be transmitted through a network **22**, or alternatively may be securely stored on an electronic storage device (not shown) for example.

Examples of suitable types of data include, but are not limited to, video stream data and/or audio stream data on substantially any type of platform such as network transmission, satellite and other wireless transmission, cable transmission, xDSL and so forth; voice communication data such as voice over IP (Internet Protocol) networks and/or through cable modems, and so forth; video stream data which has been compressed according to a particular compression method such as a member of the MPEG (Motion Picture Expert Group) set of compression methods; DVB data playback and real-time playing; and wireless transmissions such as through cellular telephones, for example.

One preferred but exemplary implementation of system **10** would be for video on-demand applications, in which a subscriber individually orders a particular video to be displayed at the request of the subscriber. System **10**

provides a mechanism for protecting the video data with encryption, in order to prevent unauthorized users from obtaining such video data.

The increased efficiency of the system and method of the present invention can be calculated according to a "gain factor", which quantifies the order of magnitude of improvement for the rate of encryption according to the present invention. For these calculations, the required numbers of instructions per bit for various encryption methods are assumed to be as follows: DES, 4 instructions per bit; 3DES, 12 instructions per bit; MD5, 0.5 instructions per bit. Therefore, implementing 3DES results in the performance of 512 x 12 instructions per block of data, or 6144 instructions.

For real-time encryption applications according to the present invention, assuming that a weaker encryption method is used for the majority of the block, while the strong encryption method is used for only 64 bits of the block, then the total number of instructions per block for the method of the present invention is 4.5 x (512-64) + (64 x 12) = 2784 instructions per block. Therefore, the gain factor in terms of numbers of instructions per block is 2784/6144 = 2.2. Thus, clearly the method and system of the present invention are significantly faster and more efficient than background art methods for real-time encryption applications.

It will be appreciated that the above descriptions are intended only to serve as examples, and that many other embodiments are possible within the spirit and the scope of the present invention.

WHAT IS CLAIMED IS:

1. A method for encrypting data with a global key, the data being divided into a plurality of blocks, the steps of the method being performed by a data processor, the method comprising the steps of:

(a) dividing each block into at least two sub-blocks, denoted as a first sub-block and a second sub-block;

(b) combining said first sub-block with said second sub-block with a hash function to form a scrambled sub-block of data as a random key;

(c) replacing said second sub-block with said random key;

(d) encrypting said first sub-block of data; and

(e) encrypting said random key with the global key.

2. The method of claim 1, wherein step (e) is performed with a strong encryption method.

3. The method of claim 2, wherein said strong encryption method is the 3DES encryption method.

4. The method of claim 2, wherein said strong encryption method is IDEA.

5. The method of claim 2, wherein step (d) is performed with a weaker method of encryption, said weaker method of encryption being less secure than said strong encryption method.

6. The method of claim 5, wherein said weaker method of encryption is the original DES encryption method.

7. The method of claim 5, wherein the global key is a plurality of global keys, such that step (e) comprises the step of encrypting said random key with each of the plurality of global keys.

8. The method of claim 5, wherein the data is broadcast application data.

9. The method of claim 8, wherein said broadcast application data is selected from the group consisting of video stream data and audio stream data.

10. The method of claim 9, wherein said broadcast application data is transmitted through a platform selected from the group consisting of network transmission, satellite transmission, cable transmission, xDSL transmission and cellular telephone wireless transmission.

11. The method of claim 8, wherein said broadcast application data is voice data.

12. The method of claim 8, wherein said broadcast application data is compressed streamed data.

13. The method of claim 12, wherein said compressed streamed data is selected from the group consisting of video stream data and audio stream data.

14. The method of claim 1, wherein steps (a) - (d) are performed as a pre-processing procedure for storing the data to form stored data.

15. The method of claim 14, wherein said pre-processing procedure is performed to form secure data storage volumes.

16. The method of claim 14, wherein said pre-processing procedure is performed to form a snapshot of said stored data.

17. The method of claim 14, wherein said pre-processing procedure is performed for a remote back-up storage of said stored data.

18. The method of claim 14, wherein said stored data is selected from the group consisting of video stream data and audio stream data.

19. The method of claim 18, wherein said stored data is transmitted through a platform selected from the group consisting of network transmission, satellite transmission, cable transmission, xDSL transmission and cellular telephone wireless transmission.

20. The method of claim 14, wherein said stored data is voice data.

21. The method of claim 14, wherein said stored data is compressed streamed data.

22. The method of claim 21, wherein said compressed streamed data is selected from the group consisting of video stream data and audio stream data.

23. The method of claim 1, further comprising the step of:

(f) interacting with the data by a plurality of users, each user having an associated global key, such that step (e) is performed with one of a plurality of global keys.

24. The method of claim 1, wherein the data is broadcast application data.

25. A method for encrypting data with a global key, the data being divided into a plurality of blocks, the steps of the method being performed by a data processor, the method comprising the steps of:

(a) dividing each block into at least two sub-blocks, denoted as a first sub-block and a second sub-block;

(b) combining said first sub-block with said second sub-block with a hash function to form a scrambled sub-block of data as a random key;

(c) replacing said second sub-block with said random key;

(d) encrypting said first sub-block of data;

(e) selecting at least a portion of the data to form a selected portion of the data; and

(f) encrypting said random key with the global key for said selected portion of the data.

26. The method of claim 25, further comprising the step of:

(g) transmitting the data.

27. The method of claim 26, wherein the data is selected from the group consisting of compressed stream data and uncompressed stream data.

28. A system for encrypting data with a global key, the data being divided into a plurality of blocks, the system comprising:

(a) a data input device for receiving the blocks of data;

(b) a sub-block division module for dividing the blocks of data into sub-blocks;

(c) a scrambling module for performing a non-reversible function on at least one sub-block of data to form scrambled data;

(d) a random key module for replacing said at least one sub-block with said scrambled data and for encrypting said scrambled data with a random local data key; and

(e) a remainder encryption module for encrypting of said sub-blocks containing said random local data key.

Figure 1

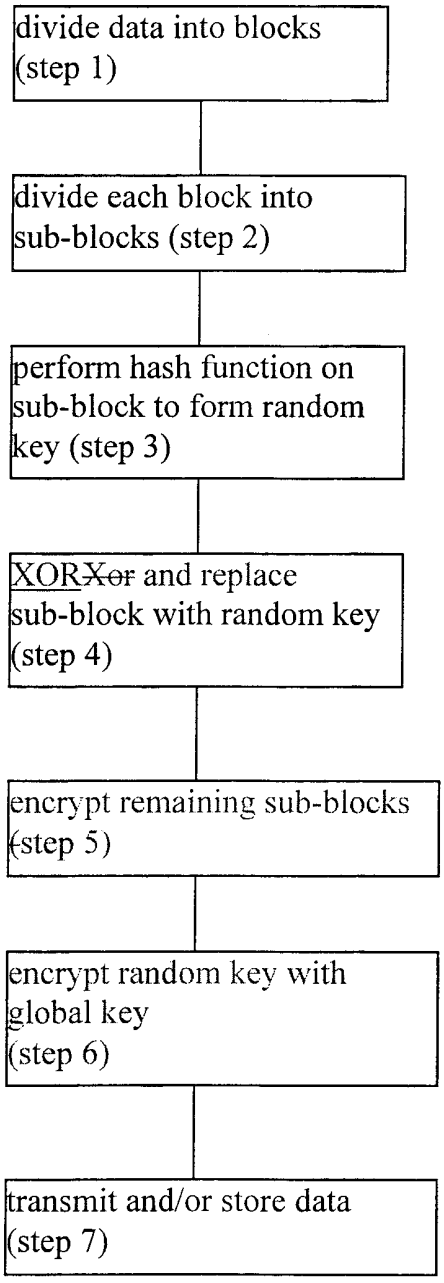

divide data into blocks (step 1)
divide each block into sub-blocks (step 2)
perform hash function on sub-block to form random key (step 3)
XORXor and replace sub-block with random key (step 4)
encrypt remaining sub-blocks (step 5)
encrypt random key with global key (step 6)
transmit and/or store data (step 7)

Figure 2

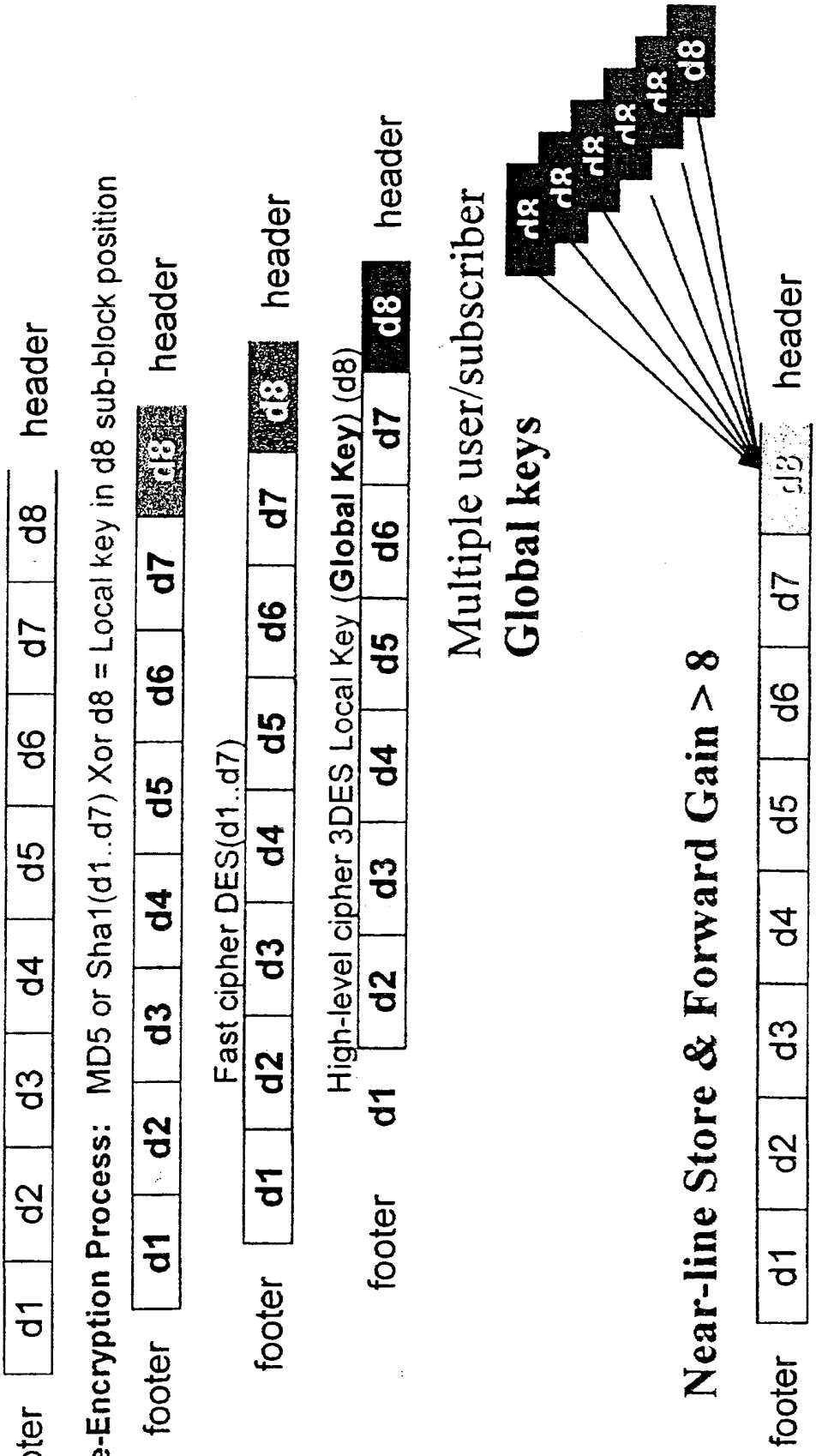
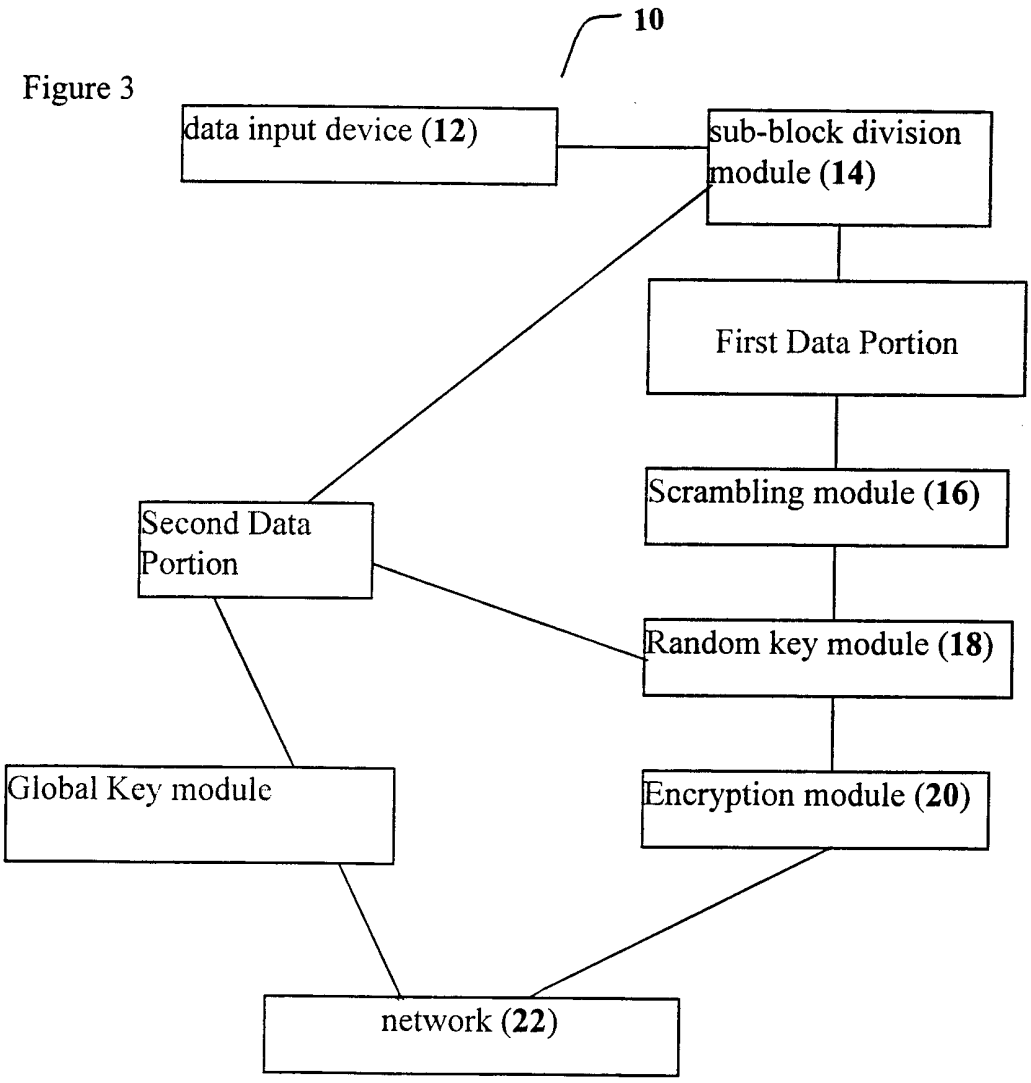

footer
d1
d2
d3
d4
d5
d6
d7
d8
header
Pre-Encryption Process: MD5 or Sha1(d1..d7) Xor d8 = Local key in d8 sub-block position
Fast cipher DES(d1..d7)
High-level cipher 3DES Local Key (Global Key) (d8)
Multiple user/subscriber
Global keys
Near-line Store & Forward Gain > 8

Figure 3


10
data input device (12)
sub-block division module (14)
First Data Portion
Scrambling module (16)
Second Data Portion
Random key module (18)
Global Key module
Encryption module (20)
network (22)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/30164

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/28
US CL : 380/28

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)
U.S. : 380/28, 37, 42, 43, 44, 46, 284; 705/51; 713/160

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,696,823 A (BLAZE) 09 December 1997 (09.12.1997), column 4, lines 12-43.	1, 2, 25, and 28
---		---
Y		3-24 and 25-27
Y	SCHNEIER, B. Applied Cryptography. Second edition. John Wiley and Sons. 1995. pages 41-43, 220-222, 319-325, and 357-366.	3-24 and 25-27
Y	US 4,484,027 A (LEE et al.) 20 November 1984 (20.11.1984), column 1, lines 5-40.	8-13, 18-22, 24, 26, and 27
A,P	US 6,052,469 A (JOHNSON et al.) 18 April 2000 (18.04.2000).	1, 25, and 28
A	US 5,987,124 A (MATYAS JR. et al.) 16 November 1999 (16.11.1999).	1, 25, and 28
A	US 5,592,553 A (GUSKI et al.) 07 January 1997 (07.01.1997).	1, 25, and 28

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent 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
15 March 2001 (15.03.2001)	09 APR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron Jr. Peggy Harwood Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)