PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
H04L 9/12

A1

(11) International Publication Number: WO 00/25476

(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/25206

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:

60/106,016	28 October 1998 (28.10.98)	US
60/122,682	3 March 1999 (03.03.99)	US

(71) Applicant: L-3 COMMUNICATIONS CORPORATION [US/US]; 34th Floor, 600 Third Avenue, New York, NY 10016 (US).

(72) Inventors: COSTANTINI, Frank; RD#2 Box 104B, Swedesboro, NJ 08085 (US). CARTER, Matthew; 3106 Ramsbury court, Mt. Laurel, NJ 08054 (US). MCGROGAN, Ellwood; 9 Blue Bell Drive, Cherry Hill, NJ 08002 (US).

(74) Agents: ROCCI, Steven, J. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, One Liberty Place – 46th Floor, Philadelphia, PA 19103 (US).

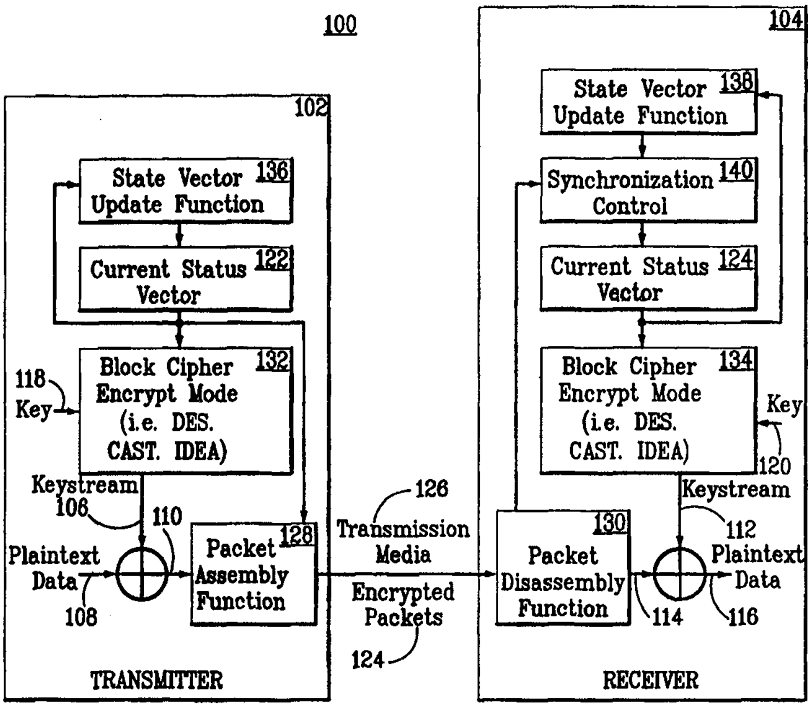
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ,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

(54) Title: APPARATUS AND METHODS FOR CRYPTOGRAPHIC SYNCHRONIZATION IN PACKET BASED COMMUNICATIONS

(57) Abstract

Apparatus (100) and methods for cryptographic synchronization in packet based communications are disclosed. A method according to the invention includes initializing a current state vector (122, 124) using the cryptographic session key (118, 120) and a cryptographic block transformation (132, 134) to produce a first keystream (106, 112), combining the first keystream with a first plaintext stream (108) to produce a first ciphertext stream (110), and updating the current state vector (122, 124) via a predefined update function (136, 138) to form an updated state vector. The update state vector can then be encrypted using the cryptographic session key (118, 120) and the cryptographic block transformation (131, 134) to produce a second keystream. The second keystream is combined with a second plaintext stream to produce a second ciphertext stream.


100
102
State Vector Update Function 136
Current Status Vector 122
Block Cipher Encrypt Mode (i.e. DES. CAST. IDEA) 132
118
Key
Keystream 106
110
Plaintext Data
108
Packet Assembly Function 128
TRANSMITTER
126
Transmission Media
Encrypted Packets
124
104
State Vector Update Function 138
Synchronization Control 140
Current Status Vector 124
Block Cipher Encrypt Mode (i.e. DES. CAST. IDEA) 134
Key
120
Keystream
112
130
Packet Disassembly Function
114
Plaintext Data
116
RECEIVER

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

APPARATUS AND METHODS FOR CRYPTOGRAPHIC SYNCHRONIZATION IN PACKET BASED COMMUNICATIONS

Field of the Invention

The present invention relates generally to cryptographic systems. More particularly, the present invention relates to apparatus and methods for cryptographic synchronization in packet based communications.

Background of the Invention

Historically, packet-based communications utilizing a stream cipher have employed one of two basic cryptographic operating modes for a block cipher as defined in FIPS 81: Output Feedback and Cipher Feedback. Either of these modes requires the sending of the entire state vector, which is typically between 64 and 256 bits, from the transmitter to the receiver, using additional communication channel overhead. Additionally, any bit errors occurring in the state vector transmission will result in either the entire packet becoming unreadable (for output feedback mode) or a large portion of the packet becoming unreadable (for cipher feedback mode). Cipher feedback mode also has the undesirable property that a single bit error occurring during transmission of a message is extended to cause errors in many bits of the received plaintext.

It would be advantageous to manufacturers of cryptographic systems, therefore, if apparatus and methods existed that require little communications overhead, support late entry participants, tolerate lost packets, tolerate bit errors in the communications channel, and ensure that state vectors are not reused. Thus, there is a need in the art for an improved cryptographic synchronization system wherein only a portion of the current state vector is sent over the network with each packet of encrypted data.

Summary of the Invention

The present invention satisfies these needs in the art by providing apparatus and methods for cryptographic synchronization in packet based communications. According to the inventive method, a current state vector in a transmitter is initialized to a predefined initialization value, such as all zeros. A cryptographic session key is generated, and the current state vector is encrypted using the cryptographic session key and a cryptographic block transformation to produce a first keystream. The first keystream is then combined with a first plaintext stream to produce a first ciphertext stream. The current state vector is updated via a predefined update function to form an updated state vector. The predefined update function can be a binary counter, for example, or a linear sequence generator.

The updated state vector is then encrypted using the cryptographic session key and the cryptographic block transformation to produce a second keystream. The second keystream is then combined with a second plaintext stream to produce a second ciphertext stream.

The ciphertext stream can then be packetized to form a packet. The packet can then be transmitted over a transmission medium to a receiver. According to one aspect of the invention, the packet can include a portion of the current state vector to be used for synchronization at the receiver.

At the receiver, as at the transmitter, a current state vector is initialized to a predefined initialization value, and a cryptographic session key is generated. The current state vector is encrypted using the cryptographic session key and a cryptographic block transformation to produce a first keystream. The first keystream is then combined with a first ciphertext stream to produce a first plaintext stream. The current state vector is updated via a predefined update function to form an updated state vector.

The updated state vector is then encrypted using the cryptographic session key and a cryptographic block transformation to produce a second keystream. The second keystream is combined with a second ciphertext stream to produce a second plaintext stream.

According to one aspect of the invention, a packet can be received from the transmitter via a transmission medium. The packet includes an encrypted payload, and can be disassembled to form the ciphertext stream from the encrypted payload. The same or a different packet can include at least a portion of a transmitter state vector. The receiver maintains synchronization with the transmitter by comparing the received portion of the transmitter state vector with a corresponding portion of the current state vector. If the corresponding portion of the current state vector differs from the received portion of the transmitter state vector, the corresponding portion of the current state vector is set to the value of the received portion of the transmitter state vector.

Apparatus for cryptographic synchronization in packet based communications can include a microprocessor adapted to perform the acts of a method described above. Similarly, the inventive method can be implemented as a set of computer executable instructions stored on a computer readable medium, such as a floppy disk, hard disk, or the like.

Brief Description of the Drawings

The foregoing summary, as well as the following detailed description of the preferred embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, there is shown in the drawings an embodiment that is presently preferred, it being understood, however, that the invention is not limited to the specific apparatus and methods disclosed.

Figure 1 is a block diagram of a packet encryption system according to the present invention.

Figure 2 depicts a preferred format for an encrypted packet in accordance with the present invention.

Detailed Description of Preferred Embodiments

Figure 1 is a block diagram of a packet encryption system 100 according to the present invention. A stream cipher cryptographic system according to the present invention includes a transmitting party transmitter 102 and a receiving party receiver 104. According to the inventive method, a stream cipher can be constructed using either a pure stream cipher keystream generator, or with a block cipher, such as Data Encryption Standard (DES), operated in a stream cipher mode. In either approach, the stream cipher generates a pseudorandom keystream. In transmitter 102, for example, keystream 106 is modulo-2 added to plaintext 108 to obtain ciphertext 110. Similarly, in receiver 104, keystream 112 is modulo-2 added to ciphertext 114 to obtain plaintext 116.

In addition to a common cipher algorithm, stream ciphers typically require that all parties share two pieces of information to provide accurate communications. First, the parties must share a cryptographic key 118, 120. Methods of deriving and/or distributing cryptographic key material are well known and are not addressed herein. The second piece of information that the two parties must share is a state vector 122, 124. A shared state vector ensures that transmitter 102 and receiver 104 are in the same state, and therefore, will generate the same pseudorandom keystream 106, 112.

According to the inventive method, a portion of the current state vector can be sent over the network periodically, with different portions being sent on varying periods. This, coupled with an *a priori* knowledge of the format of the state vector, and the way in which it changes for each packet, results in the receiver's ability to determine the correct state vector to use for the decryption of each packet. This cryptographic synchronization approach requires little communications overhead, supports late entry participants, tolerates lost packets, tolerates bit errors in the communications channel, and assures that state vectors are not reused (which would degrade security).

A method according to the present invention enables the generation of state vectors used for the encryption and decryption of data packets 124 exchanged over a communications network 126. In a preferred embodiment, state vectors 122, 124 are both fixed to the same initial value (*e.g.*, all zeros) when the cryptographic session is established, or when the encryption key is changed. In transmitter 102, state vector 122 is encrypted using an n-bit block cipher 132 and cryptographic key 118. The result of this encryption, keystream 106, is an n-bit block. Keystream 106 is then modulo-2 added to an n-bit block of plaintext 108 to provide an n-bit block of ciphertext 110. State vector 122 in transmitter 102 is then updated by passing it through an update function 136. If plaintext data 108 exceeds the block size of block cipher 132, then the encryption, modulo-2 addition, and state vector update functions are repeated until the entire plaintext payload of the packet is encrypted into ciphertext 110.

Ciphertext 110 is then packetized into encrypted packets 124, and transmitted over communications medium 126. The packetization process 128 includes adding the appropriate headers to ciphertext 110 to allow routing by the transmission network. This packetization process also includes the appending of a portion of the current state vector to the packet header (or trailer) for use by the receiver to obtain or verify synchronization.

In receiver 104, the received packet has its header removed, and the received portion of the state vector is checked against the expected value to verify synchronization. Receiver 104 then performs the identical encryption as transmitter 102, resulting in the production of identical keystream 112, which is then modulo-2 added to ciphertext 114 to restore plaintext 116. The state vector 124 in receiver 104 is updated by passing it through an identical update function 138 as used in transmitter 102.

State vector update functions 136, 138 could be binary counters, for example, or state vector 124 could be clocked through a maximal-length linear sequence generator. The updated state vector becomes the current state vector for the generation of the next n-bit block of keystream 112. This process can repeat almost indefinitely provided that a state vector value is never re-used for a given cryptographic key. It should be understood that, since a typical block cipher is at least 64 bits wide, up to a 64-bit state vector counter could be used, providing on the order of 10^{18} encrypted blocks before requiring a key change.

With every packet 124, a portion of current state vector 122 is sent to receiver 104 to check synchronization. Synchronization control function 140 compares the received portion of the state vector with the expected value maintained by its own receive state vector counter. If the values disagree, this indicates that either an error occurred in the sending of the portion of state vector 122 or receiver 104 is out of sync. If less than a threshold number of consecutive state vector portions are received with incorrect count values, they are ignored, since the error is most likely due to a transmission error. In this case, receiver 104 continues to use its internally maintained state vector 124. If the number of consecutive received state vector portions in error exceeds the threshold, it is assumed that receiver 104 is out of synchronization, and then receiver 104 enters a resynchronization state. The receiver error threshold value can be optimized for a given transmission system considering the bit error rate of the transmission media.

Since receiver 104 knows the state vector modification process, transmitter 102 is not required to send state vector values with each packet. For example, transmitter 102 could send the current state vector value to receiver 104 only once every ten packets. This increases channel utilization. Also, transmitter 102 can divide the state vector into portions, and send only a portion of the current state vector with those packets carrying state information. Since all portions of the state vector are sent within a given number of packets, this allows a late-entry recipient to also obtain synchronization within a corresponding period of time. Lost/missing packets are also accommodated since the receiver will detect an out-of-sync condition and regain sync using the subsequently received state vector information.

A further advantage of this mode of operation is that the keystream can be prepared by both the transmitter and the receiver well in advance of the actual plaintext data being available. This provides a significant advantage when the data is time-critical (such as packetized voice information), since the only delay added to the signal path due to the encryption is the small amount of time necessary to perform a simple modulo-2 addition.

Another advantage is that the block cipher need only be operated in the encrypt mode. Block ciphers typically operate in one fashion for encrypt and a reversed fashion for decrypt. If a specific implementation was required to perform both encrypt and decrypt cipher modes (as would be the case for electronic codebook mode encryption) more microprocessor / microcontroller memory resources would be required to store the programming sequence necessary to implement both modes.

In the preferred embodiment, all functions described above are performed in a single digital signal processor (DSP) device. This DSP device would produce the plaintext data (which may be derived from processing voice samples), perform the block cipher algorithm, maintain and update the state vector, perform the modulo-2 addition of keystream and plaintext, assemble the ciphertext into a packet suitable for transmission, and provide the packet to a transmission media.

In a preferred embodiment, the packets provided to the transmission media would take the form as shown in Figure 2. For packets received from the far-end party, the DSP would disassemble the packet, verify synchronization, perform the block cipher algorithm, update the state vector, perform the modulo-2 addition of keystream to ciphertext, and process the resulting plaintext as necessary.

The format of packet 150, as shown in Figure 2, begins with a pseudorandom number (PN) code 152, which the receiver uses to determine the packet boundaries. A routing header 154 is used by the transmission network to direct the packet to the proper recipient(s). Routing header 154 could take many formats, depending on the specific requirements of the transmission network. A sync control field 156 sends a portion of the state vector used for the encryption of packet 150. Preferably, sync control field 156 includes two subfields. The first subfield indicates which portion of the state vector is included in the second subfield. An encrypted payload field 158 includes the ciphertext to be securely conveyed over the network.

Other implementations and applications of this invention are also envisioned. For example, it is anticipated that a hardware device, such as a application-specific integrated circuit (ASIC), could be designed to implement the security functions described above. Likewise, a standard microprocessor or microcontroller device could be programmed to perform similar functions.

Thus there have been described apparatus and methods for cryptographic synchronization in packet based communications.. Those skilled in the art will appreciate that numerous changes and modifications may be made to the preferred embodiments of the invention and that such changes and modifications may be made without departing from the spirit of the invention. It is therefore intended that the appended claims cover all such equivalent variations as fall within the true spirit and scope of the invention.

We claim:

1. A method for cryptographic synchronization in packet based communications, comprising:

initializing a current state vector to a predefined initialization value;

generating a cryptographic session key;

encrypting the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream;

combining the first keystream with a first plaintext stream to produce a first ciphertext stream; and

updating the current state vector via a predefined update function to form an updated state vector.

2. The method of claim 1, further comprising:

encrypting the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream; and

combining the second keystream with a second plaintext stream to produce a second ciphertext stream.

3. The method of claim 1, wherein the predefined update function is a binary counter.

4. The method of claim 1, wherein the predefined update function is a linear sequence generator.

5. The method of claim 1, further comprising:

packetizing the ciphertext stream to form a packet; and

transmitting the packet over a transmission medium to a receiver.

6. The method of claim 5, wherein the packet includes a portion of the current

state vector.

7. A method for cryptographic synchronization in packet based communications, comprising:

initializing a current state vector to a predefined initialization value;

generating a cryptographic session key;

encrypting the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream;

combining the first keystream with a first ciphertext stream to produce a first plaintext stream; and

updating the current state vector via a predefined update function to form an updated state vector.

8. The method of claim 7, further comprising:

encrypting the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream; and

combining the second keystream with a second ciphertext stream to produce a second plaintext stream.

9. The method of claim 7, wherein the predefined update function is a binary counter.

10. The method of claim 7, wherein the predefined update function is a linear sequence generator.

11. The method of claim 7, further comprising:

receiving a packet that includes an encrypted payload; and

disassembling the packet to form the ciphertext stream from the encrypted payload.

12. The method of claim 7, further comprising:

receiving a packet that includes at least a portion of a transmitter state vector.

13. The method of claim 12, further comprising:

comparing the received portion of the transmitter state vector with a corresponding portion of the current state vector; and

if the corresponding portion of the current state vector differs from the received portion of the transmitter state vector, setting the corresponding portion of the current state vector to the value of the received portion of the transmitter state vector.

14. Apparatus for cryptographic synchronization in packet based communications, comprising a computer readable medium having stored thereon computer executable instructions for:

initializing a current state vector to a predefined initialization value;

generating a cryptographic session key;

encrypting the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream;

combining the first keystream with a first plaintext stream to produce a first ciphertext stream; and

updating the current state vector via a predefined update function to form an updated state vector.

15. Apparatus according to claim 14, wherein the computer readable medium has stored thereon computer executable instructions for:

encrypting the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream; and

combining the second keystream with a second plaintext stream to produce a second ciphertext stream.

16. Apparatus for cryptographic synchronization in packet based communications, comprising:

a microprocessor adapted to initialize a current state vector to a predefined initialization value, to generate a cryptographic session key, to encrypt the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream, to combine the first keystream with a first plaintext stream to produce a first ciphertext stream, and to update the current state vector via a predefined update function to form an updated state vector.

17. Apparatus according to claim 16, wherein the microprocessor is further adapted to encrypt the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream, and to combine the second keystream with a second plaintext stream to produce a second ciphertext stream.

18. Apparatus for cryptographic synchronization in packet based communications, comprising a computer readable medium having stored thereon computer executable instructions for:

initializing a current state vector to a predefined initialization value;

generating a cryptographic session key;

encrypting the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream;

combining the first keystream with a first ciphertext stream to produce a first plaintext stream; and

updating the current state vector via a predefined update function to form an updated state vector.

19. Apparatus according to claim 18, wherein the computer readable medium has stored thereon computer executable instructions for:

encrypting the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream; and

combining the second keystream with a second ciphertext stream to produce a second plaintext stream.

20. Apparatus for cryptographic synchronization in packet based communications,

comprising:

a microprocessor adapted to initialize a current state vector to a predefined initialization value, to generate a cryptographic session key, to encrypt the current state vector using the cryptographic session key and a cryptographic block transformation to produce a first keystream, to combine the first keystream with a first ciphertext stream to produce a first plaintext stream, and to update the current state vector via a predefined update function to form an updated state vector.

21. Apparatus according to claim 20, wherein the microprocessor is further adapted to encrypt the updated state vector using the cryptographic session key and the cryptographic block transformation to produce a second keystream, and to combine the second keystream with a second ciphertext stream to produce a second plaintext stream.

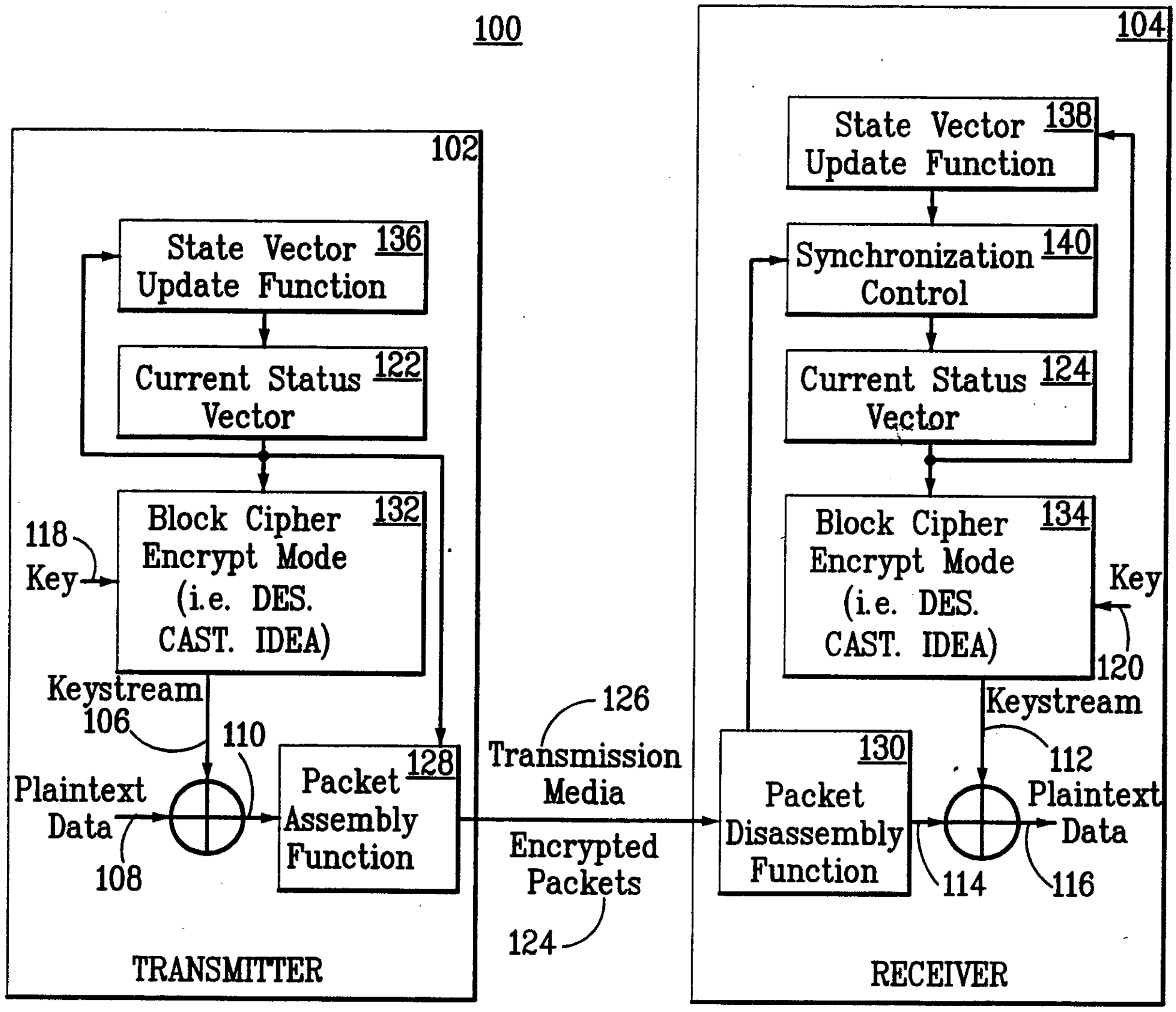

100
102
State Vector Update Function 136
Current Status Vector 122
Block Cipher Encrypt Mode (i.e. DES. CAST. IDEA) 132
118
Key
Keystream
106
110
Plaintext Data
108
Packet Assembly Function 128
TRANSMITTER
126
Transmission Media
Encrypted Packets
124
104
State Vector Update Function 138
Synchronization Control 140
Current Status Vector 124
Block Cipher Encrypt Mode (i.e. DES. CAST. IDEA) 134
Key
120
Keystream
112
Packet Disassembly Function 130
Plaintext Data
114
116
RECEIVER

FIG. 1

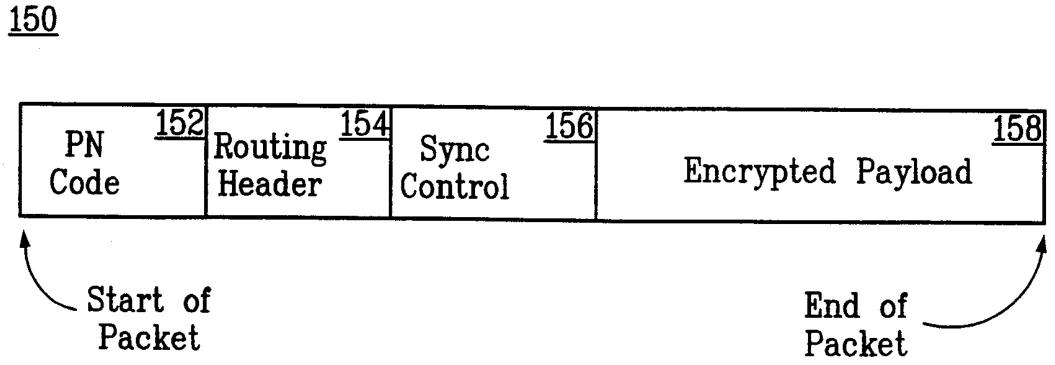

150
PN Code 152
Routing Header 154
Sync Control 156
Encrypted Payload 158
Start of Packet
End of Packet

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25206

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/12
US CL : 380/262, 284
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. : 380/262, 284, 283, 278, 260

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)

WEST/BRS: (session adj key), (initializ$ adj3 vector), (state adj vector), (stream adj cipher$1), initialization, synchronization, portion$1

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,211,891 A (GLITZ) 08 July 1980, column 2, lines 22-31.	1-21
Y	US 5,351,300 A (QUISQUATER et al.) 27 September 1994, column 1, lines 8-19.	1-21
A	US 4,856,063 A (MCCALMONT) 08 August 1989, column 2, lines 5-30.	1-21
Y	US 5,809,147 A (DE LANGE et al.) 15 September 1998, column 4, lines 32-47	1-21
Y	US 5,724,427 A (REEDS, III) 03 March 1998, column 5, lines 45-67.	1-21

□ 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 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

31 JANUARY 2000

Date of mailing of the international search report

23 FEB 2000

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 BARRÓN

Telephone No. (703) 305-3800/4700