



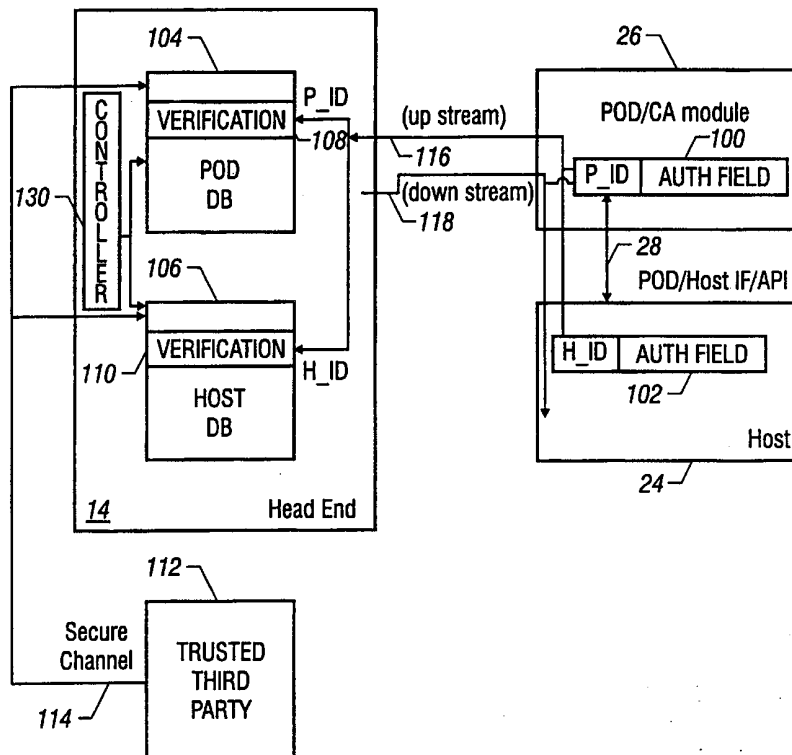
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 9/32, H04N 7/16		A1	(11) International Publication Number: WO 00/51287
			(43) International Publication Date: 31 August 2000 (31.08.00)
(21) International Application Number: PCT/US00/00713 (22) International Filing Date: 12 January 2000 (12.01.00) (30) Priority Data: 09/259,426 26 February 1999 (26.02.99) US (63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 09/259,426 (CON) Filed on 26 February 1999 (26.02.99) (71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): TAKAHASHI, Richard, J. [US/US]; 14033 South 35th Place, Phoenix, AZ 85044 (US). ZHANG, Minda [CN/US]; 3 Patten Lane, Westford, MA 01886 (US). (74) Agent: TROP, Timothy, N.; Trop, Pruner, Hu & Miles, P.C., 8554 Katy Freeway, Suite 100, Houston, TX 77024 (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, MA, 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, US, 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.	

(54) Title: PROTECTING INFORMATION IN A SYSTEM

(57) Abstract

A method and apparatus of securely communicating content between a first device (24) and a second device (26) includes sending identification information of the first and second devices to a third device (14). The third device (14) generates a predetermined message based on the identification information. The first and second devices (24, 26) are authenticated using the predetermined message.



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

Protecting Information In A System

Background

The invention relates to protection of information in a system.

Television programming and associated data may be broadcast over a number of different transport media, which may include cable networks, digital satellite television links, and other wired or wireless links. Paid television broadcasts, in which consumers pay for specific programs or channels that they would like to view (e.g., movie channels, pay-per-view programs, etc.), have become increasingly popular. To provide pay television services, conditional access systems have been used by broadcasters to enable viewing of such paid television broadcasts by authorized viewers.

In conditional access systems, broadcast programming content is typically encrypted according to some conditional access cryptographic protocol. In addition, an authorization process typically is performed to enable receipt of encrypted content by authorized receivers. The authorization process may include sending instructions to each of a potentially large population of addressable receivers (such as those located in set-top boxes, for example).

Authorization may be performed by sending an authorization signal that is targeted, or addressed, to a receiver along with the encrypted content. The authorization signal enables the addressed receiver to decrypt the encrypted content according to a conditional access protocol so that a clean copy of the programming content may be produced for viewing.

However, the encrypted information transmitted in a conditional access system may be circumvented relatively easily by unauthorized descramblers. Such unauthorized access causes loss of revenue to service providers as well as degradation of transmitted signals due to extra unexpected loading. Thus a need exists for an improved protection scheme for broadcast signals or other transmitted information.

Summary

In general, according to one embodiment, a method of securely communicating content between a first device and a second device includes sending identification information of the first and second devices to a third device. The third device generates a predetermined message based on the identification information. The first and second devices are authenticated using the predetermined message.

- 2 -

Other features and embodiments will become apparent from the following description and from the claims.

Brief Description Of The Drawings

Fig. 1A is a block diagram of an embodiment of an information transmission system.

Fig. 1B is a block diagram of a receiver according to an embodiment in the system of Fig. 1A.

Fig. 2 illustrates communications paths and stored information in the system of Fig. 1A.

Figs. 3A-3B are a flow diagram of a process according to an embodiment of protecting communication in the system of Fig. 1A.

Fig. 4 is a state diagram of the process of Figs. 3A-3B that utilizes a discrete logarithmic version of a public-key cryptographic protocol according to one embodiment.

Fig. 5 is a state diagram of the process of Figs. 3A-3B that utilizes a one-way hash function cryptographic protocol according to another embodiment.

Figs. 6 and 7 are state diagrams of the process of Figs. 3A-3B according to further embodiments that utilize a digital signature protocol to perform entity authentication and a key exchange cryptographic protocol to derive session keys.

Detailed Description

In the following description, numerous details are set forth to provide an understanding of the present invention. However, it is to be understood by those skilled in the art that the present invention may be practiced without these details and that numerous variations or modifications from the described embodiments may be possible.

In this description, the following terminology may be used. A message to be encrypted may be referred to as plaintext and an encrypted message may be referred to as ciphertext. The process of turning ciphertext back into plaintext may be referred to as decryption. The technique of keeping messages secure may be referred to as cryptography, and the technique of breaking ciphertext may be referred to as cryptanalysis. Thus, plaintext is encrypted to produce ciphertext, which is then decrypted to produce the original plaintext. A cryptographic algorithm, also referred to as a cipher, is a mathematical function or functions used for encryption and decryption. With some cryptographic algorithms, there

- 3 -

may be two related functions: one for encryption and the other for decryption. Many types of cryptographic algorithms exist, including the public-key algorithms (also referred to as asymmetric algorithms) that are designed so that the key used for encryption is different from the key used for decryption. In systems implementing public-key algorithms, the encryption
5 key may be referred to as the public key and the decryption key may be referred to as a private key (also referred to as a secret key). Other cryptographic algorithms include key-exchange algorithms, and algorithms that use one-way hash functions.

One cryptographic technique uses a session key to encrypt and decrypt communications. A session key is generally used for only one or a limited number of
10 communication sessions and then discarded. Using separate keys for different communications make it less likely that the key may be compromised.

Referring to Fig. 1A, an information transmission system may be a broadcast system (e.g., television programming or other type of video broadcast system) that includes a service provider 10 and a number of receiving sites 12 (e.g., homes that receive TV programming).

15 In other embodiments, the information transmission system may include other types of systems, such as a system including a network (e.g., local area network, wide area network, Internet, and so forth); a system for transmitting audio signals such as a telephone network or a cellular or other wireless communications network; or any other system in which information may need to be transmitted over communications channels. In the description
20 that follows, reference is made to embodiments in which television programming or video content is transmitted to multiple receiving sites; however, it is to be understood that the invention is not to be limited in this respect, but may include others.

As illustrated in Fig. 1A, the service provider 10 may include a head-end system 14 that receives content to be transmitted (the plaintext) and applies an encryption algorithm
25 according to some information protection protocol (e.g., a conditional access protocol) to produce encrypted information (the ciphertext). The encrypted information may be transmitted over a transport medium 15, such as a cable link 16, a satellite link 18, a telephone line, a terrestrial link, a wireless link, and so forth. The transmitted information is received by one or more receivers 20 located at corresponding receiving sites 12. Each
30 receiver 20 is adapted to decrypt the received information according to a specified protection protocol, such as a conditional access protocol, to reproduce the original programming content (the plaintext) for display by one or more display units 22.

- 4 -

The receiver 20 may include a host device 24, which may be an integrated receiver device (IRD) such as a set-top box, that is coupled to a point-of-deployment (POD) module 26, such as a conditional access module (CAM). The POD module 26 may be an integrated circuit card (e.g., a smart card) or other electronics device that may be inserted into a slot of, or otherwise electrically coupled to, the host device 24. To protect information communicated between the POD module 26 and the host device 24, a copy or content protection (CP) protocol may be implemented, as described further below.

The POD module 26 in the receiver 20 may be preprogrammed to decrypt certain types of transmitted information (including content encrypted according to a conditional access protocol) and to decode authorization messages, if any, transmitted by the service provider 10. Other types of host devices 24 may include a television, a video cassette recorder (VCR), a personal computer, or other devices that have integrated receivers to receive information from the head-end system 14.

The encrypted information transmitted by the head-end system 14 over the link 15 is received by the POD module 26 in the receiver 20. Based on whether the particular receiver 20 has been authorized to descramble the received information (based on an authorization message, for example), the POD module 26 may decrypt the received signal to produce plaintext. An authorization message may be sent by the head-end system 14 to the receiver 20, for example, in response to a user request to view a particular program or channel at a receiving site 12.

To protect information according to some embodiments of the invention, a copy or content protection (CP) scheme may be employed in the receiver 20 to prevent or reduce the likelihood that an unauthorized user can gain access to the information transmission system.

To prevent unauthorized access, a content protection scheme utilizes a cryptographic protocol to protect information transmitted over the link 28 between the POD module 26 and the host device 24 in the receiver 20. To verify identities of the POD module 26 and host device 24, entity authentication is performed between the POD module 26 and the host device 24 based on special binding messages transmitted by the head-end system 14. In addition, using such messages from the head-end system 14, the POD module 26 and the host device 24 can generate a session key for encrypting and decrypting messages transmitted between the POD module 26 and host device 24. Effectively, the content protection scheme bridges or links an existing conditional access system (including the head-end system 14 and

- 5 -

the POD module 26) to the copy protection system implemented in the receiver 20 (including the POD module 26 and host device 24).

Thus, according to an embodiment, to enable authentication between the POD module 26 and the host device 24, a third entity is involved, in this case the head-end system 14. The head-end system 14 may store one or more databases containing information from which the special binding messages are generated for the devices 24 and 26. The binding messages may be generated by the head-end system 14 in response to a request from the receiver 20 for a conditional access-content protection binding service (which includes performing entity authentication and session key derivation). A random counting mechanism may also be embedded in the authentication process to make it more robust against a “man-in-the-middle” and a replay attack in which messages transmitted between the POD module 26 and the host device 24 may be monitored by an intruder to break the cipher of the content protection scheme utilized in the receiver 20. Once entity authentication has been performed to ensure that the POD module 26 and the host device 24 are both verified units, a shared session key may then be derived to protect messages between the POD module 26 and host device 24.

The content protection system according to some embodiments utilizes one of many available cryptographic protocols that allow a relatively low cost implementation. Cryptographic protocols that may be used include a public-key algorithm (e.g., the ElGamal message authentication code); a one-way hash function algorithm (e.g., a secure hash algorithm such as SHA-1); and a key exchange algorithm (e.g., the Diffie-Hellman algorithm). Other types of cryptographic protocols may also be used, such as the Rivest-Shamir-Adleman (RSA) algorithm (a public-key algorithm); the Digital Signature Algorithm (a public-key algorithm); a message digest algorithm such as MD4 or MD5 (one-way hash functions); and other algorithms. The listed algorithms along with many other types of cryptographic algorithms that may be used in some embodiments of the invention are described in Bruce Schneier, “Applied Cryptography,” John Wiley & Sons, Inc. (2d ed., 1996).

Referring to Fig. 2, the entity authentication process utilized by some embodiments of the invention employs a trusted third party 112 that is able to pass either the public or secret keys of the one or more host devices 24 and POD modules 26 at one or more receiving sites 12 to the head-end system 14 over a secure channel 114. As examples, such a trusted third party may be Cable Television Laboratories Inc. (CableLabs) or some other multiple system

- 6 -

operator (MSO). The trusted third party 112 generates a list or lists of public or private keys (and/or other verification information) that are associated by device identifiers (e.g., serial numbers) of the POD modules 26 and host devices 24. The list or lists may be communicated to the head-end system 14 over a secure channel 114. From the lists, the head-end system 14 may generate one or more databases that are stored in storage media in the head-end system. For example, in the illustrated embodiment, the head-end system 14 includes a database 104 to store verification information associated with POD modules 26 and a database 106 to store verification information associated with host devices 24. The one or more databases are accessed by the head-end system 14 to generate binding messages for a host device 24 and a POD module 26, and in some embodiments, to verify identities of the host device and POD module during the entity authorization process. Once entity authentication has been performed, the POD module 26 and host device 24 may further generate session keys (which may also be based on the binding messages sent by the head-end system) to protect communications with each other.

In this description, the information transmission system may also be referred to as a conditional access/content protection (CA-CP) system. The CA-CP system according to an embodiment may include a number of components, including the head-end system 14 that is part of a conditional access system that sets up and encrypts content for transmission over the transport medium 15. The head-end system 14 also stores one or more databases (e.g., 104 and 106) containing verification information of the devices 24 and 26. Another component of the CA-CP system is the transport medium 15 to allow two-way communication (over an upstream path 116 and a downstream path 118) between the head-end system 14 and the receiver 20. On the two-way communications link 15, the receiver 20 can request that the head-end system 14 provide a CA-CP binding service according to an embodiment to allow the devices 24 and 26 to perform entity authentication. Downstream communication over the path 118 from the head-end system 14 to the receiver 20 includes protected content transmitted under a conditional access protocol as well as messages that are generated as part of the CA-CP binding service.

After entity authentication and session key derivation have been performed, the POD module 26 can decrypt ciphertext received from the head-end system 14 according to a CA protocol to produce a clean copy of the transmitted content. The POD module 26 next encrypts the clean content using a session key derived according to the CP protocol before

- 7 -

transmission to the host device 24, which decrypts the transmitted information using the session key stored in the host device 24. The interface between the host device 24 and the POD module 26 may be an open application programming interface (API).

Referring further to Fig. 3, the process of performing the entity authentication and session key derivation (also referred to as a binding service) is illustrated. The receiver 20 transmits (at 302) authorization fields (or portions of authorization fields) of both the host device 24 and the POD module 26 over the upstream path 116 of the transport medium 15 to the head-end system 14. A POD authorization field 100 in the POD module 26 may include the device identifier P_ID of the POD module 26 along with other information (as described below), and a host authorization field 102 in the host device 24 may include the device identifier H_ID of the host 24 along with other information. The authorization fields 100 and 102 (or portions of such authorization fields) transmitted to the head-end system 14 effectively provide a request to the head-end system to perform a binding service (including entity authentication and session key derivation). In other embodiments, a separate message or a predefined flag or other indication may constitute a request to start a binding service.

A controller 130 in the head-end system 14 uses the device identifiers P_ID and H_ID in the received authentication field portions to map into corresponding locations in the databases 104 and 106, respectively (at 304). In one embodiment, the controller 130 may be implemented as a combination of hardware and software. The hardware may include, for example, a processor such as a microprocessor, microcontroller, a finite state machine implemented as an application specific integrated circuit (ASIC) or a programmable gate array (PGA), and the like. The hardware may also include one or more storage elements. Software in the head-end system 14 may include one or more routines to perform conditional access operations as well as generation of binding messages in response to requests from one or more receivers 20.

The identifier P_ID maps into a location 108 in the POD database 104, and H_ID maps into a location 110 in host database 106. Verification information stored in locations 108 and 110 of the POD database 104 and host database 106, respectively, may include one or more of the following items associated with the POD module 26 and the host device 24: a private or secret key; a public key; a predetermined signature; or other verification information. The verification information stored in the POD and host databases 104 and 106 may be used by the head-end controller 130 to generate binding messages for the requesting

- 8 -

receiver 20, and optionally, to confirm that the authorization fields actually originated from authorized devices 24 and 26. Verification may be performed simply by checking that verification information associated with the devices 24 and 26 of the requesting receiver 20 is stored in the databases 104 and 106. Alternatively, verification may be performed by
5 comparing contents of the received authorization field portions with verification information stored in locations 108 and 110 of the databases 104 and 106, respectively. If the head-end controller 130 is able to verify (at 306) the devices 24 and 26, the head-end system 14 next sends (at 308) binding messages over the downstream path 118 of the transport medium 15 to the POD module 26. If the head-end system 14 is unable to verify the at least one device 24
10 or 26 of a requesting receiver 20, then a predetermined error message may be sent (at 310).

From the binding messages sent by the head-end system 14, the POD module 26 determines (at 312) if the host device 24 is an authorized device. If the authentication is successful, then the POD module 26 transmits (at 316) binding information to the host 24 and generates and stores (at 318) the session key to use in protection of communications between
15 the POD module 26 and host device 24. However, if the POD module 26 is unable to authenticate the host device, then an error message may be generated (at 314).

In the host device 24, the received binding information is used to authenticate the POD module 26 (at 320). If authentication is unsuccessful, then an error message may be generated (at 322). However, if authentication is successful, then the host device 24
20 generates and stores (at 324) the session key to use to decrypt content received by the POD module 26. Using the independently derived session key stored separately in the POD module 26 and the host device 24, secure communications over the link 28 in the receiver 20 may be performed (at 324). The session keys are stored in secure storage elements in the host device 24 and POD module 26 that are tamper-resistant.

Thus, as described, the host device 24 and POD module 26 are able to authenticate
25 each other based on binding messages transmitted by the head-end system 14 to the host device 24 and POD module 26. By using the binding process according to some embodiments of the invention, system integrity may be maintained by reducing the likelihood that the protection protocol used can be circumvented by unauthorized users and devices. In
30 addition, the authentication may be performed independently of whatever conditional access mechanism may be utilized by the head-end system 14. Further, some embodiments of the

invention allow a relatively low computation burden for the POD module 26 and the host device 24 during the binding process.

Referring to Fig. 1B, components and layers of the host device 24 and the POD module 26 are illustrated. Each of the host device 24 and POD module 26 includes a link interface 200 and 202, respectively, that are coupled to the link 28. In one example, the link interface 200 in the host device 24 may be coupled to a slot to receive the POD module 26, which may be an electronic card such as a smart card. The host device 24 and POD module 26 also include control devices 204 and 206, respectively, to control operations of the respective devices. Control routines 205 and 207 stored in respective storage elements may be executable on the control devices 204 and 206, respectively, to perform various tasks. In the POD module 26, the control routine 207 may perform decryption of conditional access ciphertext transmitted from the head-end system 14, entity authentication and session key derivation according to the binding service, and encryption of content according to a content protection protocol for transmission over the link 28. In the host device 24, the control routine 205 may perform entity authentication and session key derivation according to the binding service, decryption of content received over the link 28, and processing of the decrypted content (including for display and/or other manipulation).

Storage elements 208 and 210 are also included in the devices 24 and 26, respectively, to store such information as authorization fields, binding messages originating from the head-end system 14, transmitted content from the head-end system 14, software instructions and data, and so forth. The control devices 204 and 206 may be various types of control devices, including microprocessors, microcontrollers, ASICs, PGAs, and other programmable devices. The storage elements 208 and 210 may be one or more of various types of memories, such as dynamic random access memories (DRAMs), static random access memories (SRAMs), electrically erasable and programmable read only memories (EEPROMs), flash memories, and other types of memories such as hard disk drives, floppy disk drives, compact disc (CD) and digital video disc (DVD) drives.

To perform various cryptographic operations, the host device 24 and the POD module 26 may include the following units, respectively: arithmetic processing units 212 and 214; exclusive OR (XOR) units 216 and 218; random number generators 220 and 222; and counters 224 and 226. The units 212, 216, 220, and 224 in the host device 24 may be integrated into a single programmable device, such as a control device 204, or implemented

- 10 -

as discrete units. The units 214, 218, 222, and 226 in the POD module 26 may be similarly arranged. Such units may also be implemented in software, for example, as part of the control routines 205 and 207. Alternatively, tasks performed by the control routines 205 and 207 may be performed by hardware.

5 As sensitive information may be kept in the storage elements 208 and 210 of the host device 24 and POD module 26, respectively, external access to those storage elements is prevented. Sensitive information may include the public and private keys or other information used in the binding process, as well as any derived session key for communications protected by a content protection protocol.

10 The following describes embodiments of information transmission systems that implement one of the following cryptographic algorithms for performance of the binding service: the ElGamal algorithm, which is a discrete logarithmic version of a public-key algorithm (Fig. 4); the SHA-1 algorithm, which is a one-way hash function algorithm (Fig. 5); and a combination of the Diffie-Hellman key exchange algorithm and digital signature
15 algorithm (Figs. 6-7). It is to be understood, however, that the invention is not to be limited to such described embodiments, as other types of cryptographic algorithms may also be implemented in further embodiments.

Referring to Fig. 4, a state diagram is illustrated for a protection protocol according to one embodiment that implements the ElGamal algorithm to perform entity authentication and
20 session key derivation. In the illustrated embodiment, three separate stages are included. In stage 1, setup of the content protection system including the POD module 26 and the host device 24 is performed. This may occur during initialization, such as when the POD module 26 is initially plugged into the host device 24 or when the host device 24 is power cycled. Five states are included in stage 1, in which messages are exchanged among the host device
25 24, the POD module 26, and the head-end system 14 to securely deliver information in the authorization fields of the host device 24 and the POD module 26 to the host device 24. In stage 2, entity authentication and session key derivation are performed. Three states (6, 7, and 8) are included in stage 2. Once stage 2 has been completed, communications between the POD module 26 and host device 24 may be protected according to a content protection
30 protocol, which may include a cryptographic algorithm such as a symmetric cipher algorithm that utilizes a session key separately derived and stored in the devices 24 and 26.

As illustrated in Fig. 4, the authorization field stored in the storage element 208 of the host device 24 may include its device identifier (H_ID), its private key H, its public key $G^H \bmod N$, and a random number generator (RNG) seed S_H (described below). The POD module 26 may store the following authorization field in its storage element 210: its device identifier P_ID, its private key P, its public key $G^P \bmod N$, and an RNG seed S_P . N is a predefined prime number, G is a predefined random number that serves as a generator, and mod N represents modulo N. In the head-end system 14, according to the illustrated embodiment, a reciprocal ($G^{-P} \bmod N$) of the POD module public key $G^P \bmod N$ is stored as verification information in database 104, and a reciprocal ($G^{-H} \bmod N$) of the host public key $G^H \bmod N$ is stored as verification information in the database 106.

During the set up stage (stage 1), the host device 24 generates a random number M_H in state 1 and transmits the following string $\{H_ID \parallel M_H\}$ to the POD module 26 over the link 28. As used in this description, the term "A $\parallel$ B" indicates concatenation of fields A and B in a stream. In state 2, the POD module 26 generates its random number M_P and derives a common counter value M_0 which is an exclusive OR of M_P and M_H :

$$M_0 = M_P \oplus M_H.$$

Next, the POD module 26 sends a stream containing concatenated device IDs $\{P_ID \parallel H_ID\}$, which are part of the authorization fields of the POD module 26 and host device 24, to the head-end system 14. The authorization field portions are indications to the head-end system 14 that a binding service has been requested. In state 3, based on the received values P_ID and H_ID, the head-end controller 130 accesses locations 108 and 110 in databases 104 and 106, respectively, to retrieve verification information $G^{-P} \bmod N$ and $G^{-H} \bmod N$. In state 3, the head-end controller 130 calculates the modulo multiplication of the retrieved values to obtain binding message $G^{-(P+H)} \bmod N$:

$$G^{-(P+H)} \bmod N = [G^{-P} \bmod N] [G^{-H} \bmod N] \bmod N.$$

The binding message is transmitted back to the POD module 26 over the link 15 between the head-end system 14 and the receiver 20. In state 4, the POD module 26 performs a modulo multiplication of the received value $G^{-(P+H)} \bmod N$ with its public key $G^P \bmod N$ to obtain $G^{-H} \bmod N$:

$$G^{-H} \bmod N = [G^{-(P+H)} \bmod N] [G^P \bmod N] \bmod N.$$

- 12 -

The POD module 26 then forwards the binding message $G^{-(P+H)} \bmod N$ concatenated with the random number M_P , $\{G^{-(P+H)} \bmod N \parallel M_P\}$, to the host device 24 over the link 28.

Next, in state 5, the host device 24 also independently derives the common counter value M_0 by performing the exclusive OR of M_P and M_H . In addition, the host device 24
 5 computes $G^{-P} \bmod N$ by performing the modulo multiplication of the binding message transmitted by the head-end system 14 with the host device's public key:

$$G^{-P} \bmod N = [G^{-(P+H)} \bmod N][G^H \bmod N] \bmod N$$

States 1-5 complete the setup stage in which messages, including the device IDs of the host device 24 and POD module 26, random numbers M_H and M_P , and the binding message have
 10 been exchanged among the host device 24, POD module 26, and head-end system 14.

After the setup stage, entity authentication and session key derivation are performed between the POD module 26 and host device 24 in stage 2. Once authenticated, the POD module 26 and the host device 24 are authorized to independently derive the session key according to the content protection scheme used in the receiver 20. In one embodiment, the
 15 derived session key may include a 1,024-bit entropy that is sufficient for 16 consecutive sessions to cipher content between the POD module 26 and the host device 24. In some embodiments, the content protection protocol performed in the receiver 20 utilizes a symmetric cryptographic algorithm that includes the session key.

In state 6, which is the first state of the authentication and session key derivation stage, a value M is initialized to the common counter value M_0 . Next, M is updated by
 20 incrementing it by 1 (or by some other predetermined value):

$$M \leftarrow M + 1.$$

In addition, the POD module 26 also encrypts M for the host device 24 using a modified ElGamal algorithm by generating a random integer s and computing $G^s \bmod N$ and
 25 $M(G^{-H})^s \bmod N$. The stream $\{G^s \bmod N \parallel M(G^{-H})^s \bmod N\}$ is sent from the POD module 26 to the host device 24.

Next, in state 7, the host device 24 initializes a variable M also to the common counter value M_0 . Also, M is updated by incrementing it with 1 to synchronize it by the value M in the POD module 26. The host device 24 uses the modified ElGamal algorithm to encrypt M
 30 for the POD module 26 by first generating a random integer t , and then computing $G^t \bmod N$ as well as $M(G^{-P})^t \bmod N$. The host device 24 then sends the following stream $[G^t \bmod N \parallel M(G^{-P})^t \bmod N]$ to the POD module 26. Also in state 7, the host device 24 also

- 13 -

decrypts the ciphertext sent by the POD module 26 to derive M' by performing a modulo multiplication as follows:

$$M' = \left\{ \left[M(G^{-H})^s \bmod N \right] \cdot \left(G^S \bmod N \right)^H \right\} \bmod N.$$

If the parameter M' is equal to the parameter M , then the host device 24 has authenticated the
 5 POD module 26, and the host device 24 derives the shared key k which is calculated as follows:

$$k = (G^{ts} \bmod N) = \left[(G^s \bmod N)^t \bmod N \right].$$

Next, in state 8, the POD module 26 receives the ciphertext from the host device 24 and calculates a parameter M' by performing the following operation:

$$10 \quad M' = \left\{ \left[M(G^{-P})^t \bmod N \right] \cdot (G^t \bmod N)^P \right\} \bmod N.$$

Next, the value of M' is compared to the value of M , and if equal, the POD module 26 authenticates the host device 24 and derives a shared session key k as follows:

$$k = (G^{ts} \bmod N) = \left[(G^t \bmod N)^s \bmod N \right].$$

After completion of entity authentication and shared key derivation, the final key K is
 15 calculated from the session key k under modulo of the target cipher key size:

$$K = k \bmod (\text{cipher key size}).$$

This operation circulates the data field of k up to exhaust the entropy of k .

Upon establishing the shared session key K , the POD module 26 can now cipher the content transmitted over the link 28 in the receiver 20 according to the content protection
 20 protocol. The content protection protocol to protect content transmitted between the host device 24 and POD module 26 is performed in states 9 and 10 which are included in stage 3 of the state diagram of Fig. 4. Such content may include broadcast video and audio data.

According to one embodiment, in state 9, the POD module 26 decrypts a transported stream received from the head-end system 14 according to a conditional access protocol
 25 between the head-end system 14 and the POD module 26. Next, the POD module 26 encrypts the content from the head-end system 14 using the derived session key K according to a symmetric cipher and forwards the ciphertext to the host device 24 over the link 28. Next, in the state 10, the host device 24 decrypts the ciphertext using the derived session key

- 14 -

K according to the symmetric cipher to obtain clean data that may be further processed by the host device 24 (such as for display to a viewer or other operations).

The random number generators 220 and 222 in the host device 24 and POD module 26, respectively, are adapted to generate random numbers M_H and t (in the host device 24) and M_P and s (in the POD module 26). The random numbers may be truly random or pseudo-random numbers used to enhance security by providing randomized challenges between the host device 24 and the POD module 26. In one embodiment, the random number generator (RNG) used in each of the devices 24 and 26 employs an ElGamal encryption engine as a one-way function, although other techniques of generating random numbers are also contemplated. Inputs to the random number generator 220 or 226 include an RNG seed S (S_P in the POD module 26 and S_H in the host device 24), which may be a 160-bit string, a private key K , which may also be 160 bits in length (the private key is P in the POD module 26 and H in the host device 24), and a b -bit string c , in which $160 < b < 1024$. The bit stream c may be selected in such a way that any two consecutive values are different.

The output of the random number generator 220 or 222 is a string denoted by $G(s,k,c)$, which in one embodiment may be a 1,024-bit string. In one embodiment, the random number generator 220 or 222 may generate random numbers as follows. Initially, a parameter u is defined that includes the 160 least significant bits of c :

$$u \leftarrow c_{\text{lsb-160}}.$$

Next, a message block X is created by padding the string c with zeros to obtain a 1,024-bit message block X :

$$X \leftarrow c \parallel 0^{1024-b}.$$

An exclusive OR operation is then performed on the RNG seed S and the parameter u to obtain a random number v :

$$v \leftarrow s \oplus u.$$

The ElGamal encryption step is then executed with message X , the random number v , and the private key K to obtain the message Y :

$$Y \leftarrow X(G^K)^v \bmod N.$$

The output $G(s,K,c)$ is then set equal to the encrypted message Y , which is a random number.

The output $G(s,K,c)$ is a 1,024-bit integer. In the authentication process according to some embodiments, the random number generated in the POD module 26 is the 160 least

- 15 -

significant bits of the output $G(s,P,c)_{lsb-160}$, and the random number generated in the host device 24 is the 160 least significant bits of the output $G(s,H,c)_{lsb-160}$.

According to another embodiment, one-way hash functions may be utilized in the binding service among the head-end system 14, the host device 24, and POD module 26.

5 One example of an one-way hash function algorithm is a secure hash algorithm (SHA) such as SHA-1.

Referring to Fig. 5, an entity authentication and key derivation process according to an embodiment to protect communications between the host device 24 and the POD module 26 uses a SHA-1 algorithm. The process is divided into three stages: an initialization stage (stage 1); an entity authentication and key derivation stage (stage 2); and a communications stage (stage 3) in which exchange of data between the POD module 26 and the host device 24 is protected by the derived session key.

A trusted third party 112 (Fig. 2) supplies a list of device identifiers and corresponding secret keys (e.g., 160-bit secret keys) and RNG seeds (e.g., 160-bit RNG seeds) for POD modules 26 and host devices 24 in the information transmission system. The secret keys are stored in various locations in the POD and host databases 104 and 106 that are addressable by POD device identifiers (P_IDs) and host device identifiers (H_IDs), respectively.

In this embodiment, the authorization field for the POD module 26 is represented as $\{P_ID \parallel P \parallel S_P\}$, which includes a concatenation of the POD module device identifier, secret key, and RNG seed, respectively. Similarly, the host device's authorization field is represented as $\{H_ID \parallel H \parallel S_H\}$. The secret keys P and H of the POD module 26 and host device 24 are stored in tamper-resistant storage elements 210 and 208, respectively.

During initialization, after the POD module 26 has been plugged into or otherwise operatively coupled to the host device 24, or after the host device 24 has been power cycled, the POD module 26 and host device 24 exchange newly generated random number integers N_P and N_H from the POD module 26 and host device 24, respectively. Each device then independently sets a common initial counter value $N_0 : N_0 = N_P \oplus H$.

Next, after initialization in state 1, the host device 24 sets N equal to N_0 and then increments N by one (or some other predetermined value). The host device 24 then computes $SHA-1(N \oplus H)$, which is the secure hash function of $N \oplus H$, and sends the following stream $\{H_ID \parallel SHA-1(N \oplus H)\}$ to the POD module 26. In state 2, the POD module 26 also

- 16 -

initializes N to N_0 and increments N by one (or some other value). The POD module 26 then computes the one-way hash function $\text{SHA-1}(N \oplus P)$. Next, the POD module 26 sends the following stream $\{P_ID \parallel H_ID \parallel N \parallel \text{SHA-1}(N \oplus H) \parallel \text{SHA-1}(N \oplus P)\}$ to the head-end system 14. This indicates to the head-end system 14 that a binding service has been requested. In state 3, based on the received P_ID and H_ID values, the head-end controller 130 accesses storage locations 108 and 110 in databases 104 and 106, respectively, to retrieve the secret keys P and H of the POD module 26 and host device 24, respectively. After retrieving P and H , the head-end controller 130 computes $\text{SHA-1}(N \oplus P)$ and $\text{SHA-1}(N \oplus H)$, since P , H , and N are all known in the head-end system 14. The computed SHA-1 values are compared to the received SHA-1 values. If the values match, then the POD module 26 and host device 24 are identified by the head-end system 14 as trusted players.

In state 3, the head-end controller 130 then computes the following values which are sent in a binding stream back to the POD module 26: $\text{SHA-1}[\text{SHA-1}(N \oplus H) \oplus P]$; $\text{SHA-1}[\text{SHA-1}(N \oplus P) \oplus H]$; $\text{SHA-1}(H \parallel N) \oplus \text{SHA-1}(P)$; and $\text{SHA-1}(P \parallel N) \oplus \text{SHA-1}(H)$. The former two terms are used for entity authentication and the latter two terms are used for shared key derivation. In state 4, the POD module 26 authenticates the host device 24 by computing the following hash function: $\text{SHA-1}[\text{SHA-1}(N \oplus H) \oplus P]$, from which $\text{SHA-1}(N \oplus H)$ was received from the host device 24 and P is the secret key of the POD module 26. The derived value is compared to the hash function transmitted by the head-end system 14. If a match is determined, then the POD module 26 has authenticated the host device 24. Once authenticated, the POD module 26 derives the key k :

$$k = \text{SHA-1}(H \parallel N) \oplus \text{SHA-1}(P \parallel N).$$

In the above operation, the term $\text{SHA-1}(P \parallel N)$ is derived by taking the result $\text{SHA-1}(H \parallel N) \oplus \text{SHA-1}(P)$ from the head-end system 14 and performing an exclusive OR operation of the result with the term $\text{SHA-1}(P)$.

In turn, the POD module 26 forwards a stream including the following terms to the host device 24: $\text{SHA-1}(N \oplus P)$, $\text{SHA-1}[\text{SHA-1}(N \oplus P) \oplus H]$, $\text{SHA-1}(P \parallel N) \oplus \text{SHA-1}(H)$.

In state 5, upon receiving the binding stream from the POD module 26, the host device 24 computes the following term: $\text{SHA-1}[\text{SHA-1}(N \oplus P) \oplus H]$, from which $\text{SHA-1}(N \oplus P)$ was received from the POD module 26.

- 17 -

The result is compared to the same hash function forwarded by the POD module 26 (originally from the head-end system 14). If a match is found, then the host device 24 has authenticated the POD module 26, and the host device 24 derives the shared key k :

$$k = \text{SHA-1}(H \parallel N) \oplus \text{SHA-1}(P \parallel N).$$

- 5 In the above operation, the term $\text{SHA-1}(P \parallel N)$ is derived by performing an exclusive OR operation of the following received value $\text{SHA-1}(P \parallel N) \oplus \text{SHA-1}(H)$ from the POD module 26 with the hash function $\text{SHA-1}(H)$. The result of the exclusive OR operation is the value $\text{SHA-1}(P \parallel N)$.

- 10 Once entity authentication and the shared key derivation have been performed by the POD module 26 and the host device 24, the final shared session key K is calculated by each device by taking the key k under module of the target cipher key size:

$$K = k \bmod (\text{cipher key size}).$$

Using the shared session key K , the POD module 26 can cipher the content to be transmitted to the host device 24 over the link 28.

- 15 Thus, in state 6 of Fig. 5, the POD module 26 decrypts a data stream received from the head-end system that has been encrypted using a conditional access protocol. The POD module 26 then encrypts the clean content using the session key K according to a symmetric cipher and forwards the cipher content to the host device 24 over the link 28. In state 7, the host device 24 receives the cipher content and decrypts it to obtain a clean copy of the
20 content for further processing by the host device 24.

- The random number generator (RNG) 220 or 222 (in device 24 or 26) according to this embodiment may utilize SHA-1 as a one-way hash function. In this embodiment, the random number generation may be performed according to the random number generation specification described in the Federal Information Processing Standards (FIPS) Publication
25 186, dated May 19, 1994, and available at {<http://www.itl.nist.gov>}. The input to the RNG 220 or 222 may be a 160-bit RNG seed S (S_P in the POD module 26 and S_H in the host device 24) and a b -bit string c , in which $160 < b < 512$. The output of the RNG 220 or 222 is a 160-bit string that is denoted as $G(s, c)$.

- 30 According to another embodiment, entity authentication between the POD module 26 and the host device 24 is performed using a digital signature algorithm and a session key is derived according to a Diffie-Hellman key exchange scheme.

- 18 -

Referring to Fig. 6, a state diagram of an authentication and key exchange algorithm according to another embodiment is illustrated. The authorization field in the host device 24 for this embodiment may include $\{H_ID, S_{H^{-1}}(H_ID), H, H^{-1}\}$, where H_ID is the ID of the host device 24, $S_{H^{-1}}(H_ID)$ is the digital signature of H_ID created by the private key H^{-1} of the host device 24, and H is the public key of the host device 24. The POD module 26 includes the following information in its authorization field: $P_ID; S_{P^{-1}}(P_ID); P^{-1}; P$.

Digital signature algorithms that may be used include the digital signature standard as described by the National Institute of Standards in Technology (NIST) in its Digital Signature Standard bulletin, dated January 1993. The Digital Signature Standard (DSS) is also known as the Federal Information Processing Standard (FIPS) 186. A variation of DSS is the elliptic version of DSS. Another digital signature algorithm that may be utilized is the Rivest-Shamir-Adleman (RSA) algorithm as described by RSA Data Security Inc. at their web site $\{\text{http://www.rsa.com/rsalabs/}\}$, dated in 1998.

To start the authentication process, the host device 24 sends portions of its authorization field $\{H_ID \parallel S_{H^{-1}}(H_ID)\}$ to the POD module 26 in state 1. Next, in state 2, the POD module 26 sends portions of its authorization field $\{P_ID \parallel S_{P^{-1}}(P_ID)\}$ as well as the authorization information of the host device 24 to the head-end system 14. In state 3, the head-end system 14 compares the received authorization field information with data stored in databases 104 and 106. P_ID is used to retrieve information from location 108, which stores the public key P of the POD module 26 as well as its digital signature $S_{P^{-1}}(P_ID)$. Similarly, H_ID retrieves information from location 110 in the database 106, which includes the public key H of the host device 24 as well as its digital signature $S_{H^{-1}}(H_ID)$. Thus, in state 3, the head-end system 14 verifies that the received authorization field information is from authorized devices based on a comparison to the retrieved information from locations 108 and 110.

In state 4, once the head-end system 14 verifies that the devices 26 and 24 are valid devices, the head-end system 14 encrypts the public key P of the POD module 26 using a symmetric cipher scheme with the public key H of the host device 24 to derive $E_H[P]$. A possible symmetric cipher scheme may be a block cipher scheme, a stream cipher scheme, and others.

The head-end system 14 then sends $E_H[P]$ back to the POD module 26. Upon receipt of $E_H[P]$, the POD module 26 has implicitly authenticated the host device 24. To allow the

- 19 -

host device 24 to authenticate the POD module 26, the POD module 26 sends the following stream $\{E_H[P] \parallel P_ID \parallel S_{P-1}(P_ID)\}$ to the host device 24 in state 5. This allows the host device to authenticate the POD module 26 by performing the operation $V_P[P_ID \parallel S_{P-1}(P_ID)]$ using the POD module's public key P. P is derived by the host 24 by decrypting $E_H[P]$ with the host's key H. The operation $V_p[]$ is performed by a verification engine in the host device 24 according to the digital signature algorithm.

After completion of entity authentication in states 1-5, the creation of a session key is started. In state 7, each of the POD module 26 and host device 24 generates their respective random integers x and y and computes $G^x \bmod N$ and $G^y \bmod N$, respectively, where N is a common modulus and G is a common generator. The host device 24 sends $G^y \bmod N$ to the POD module 26, and similarly, the POD module 26 sends $G^x \bmod N$ to the host device 24. In state 8, the POD module 26 calculates a shared session key k:

$k = (G^y \bmod N)^x \bmod N = G^{yx} \bmod N$. In state 8, the host device 24 takes the value received from the POD module 26 and computes the shared key k:

$k = (G^x \bmod N)^y \bmod N = G^{xy} \bmod N$. The shared session key k is used by the POD module 26 and host device 24 to protect communications over the link 28. After the POD module 26 decrypts data received from the head-end system according to the payload cipher algorithm (e.g., a conditional access algorithm), the POD module 26 then encrypts the content using the session key k and forwards the cipher content to the host device 24, which decrypts the cipher content using its copy of the session key k.

Referring to Fig. 7, to further enhance security, several additional operations may be performed in addition to those described in connection with Fig. 6. In particular, the security level upgrading may be achieved by modifying states 4 and 7 in Fig. 6.

In Fig. 7, the upgraded security scheme includes operations that may be identical to those of Fig. 6 except for states 4 and 7. In state 4* of Fig. 7, after receipt of authorization field information from the POD module 26 and the host device 24, the head-end system 14 generates both encrypted public keys: $E_H[P]$ and $E_P[H]$. Both encrypted public keys are then transmitted back to the POD module 26, which extracts the public key H of the host device from $E_P[H]$. When the stream $\{E_H[P] \parallel P_ID \parallel S_{P-1}(P_ID)\}$ is transmitted by the POD module 26 to the host device 24, the host device 24 can extract the public key P of the POD module 26 from $E_H[P]$. Since both the public and private keys of the devices 24 and 26 are

- 20 -

well protected, a middle-man attack would be unlikely to break the system during the passing of the public keys to each other over secure channels.

State 7 is modified from that of Fig. 6 by breaking it into three states 7a, 7b, and 7c. In this embodiment, both the POD module 26 and the host device 24 generate a randomized challenge x_n and y_n , as well as random integers x and y , which are used to derive the shared session key between the devices 26 and 24. In addition, in state 7a, the POD module 26 and host device 24 calculate $G^x \bmod N$ and $G^y \bmod N$, respectively. The random numbers x_n and y_n are exchanged between the POD module 26 and host device 24. In state 7b, the POD module 26 generates its digital signature on the received challenge y_n from the host device 24 by calculating a first phase Diffie-Hellman variable using the private key P of the POD module: $S_P^{-1}(y_n \parallel G^x \bmod N)$. Similarly, in state 7b, the host device 24 generates $S_H^{-1}(x_n \parallel G^y \bmod N)$. The respective digital signatures are exchanged between the POD module 26 and host device 24 along with $G^x \bmod N$ and $G^y \bmod N$. Upon receipt in state 7c, each of the POD module 26 and host device 24 verifies the signature and extracts the first phase Diffie-Hellman variables. Successful verification results in the POD module 26 and host device 24 authenticating each other. Next, in state 8, the shared session key k is derived as in the embodiment of Fig. 6.

Some embodiments of the invention may have one or more of the following advantages. Vulnerability is localized such that compromise of one device does not result in system wide compromise. To achieve that end, according to some embodiments, local cryptographic variables are used and are chosen so as to not threaten the overall system in the event of compromise. In addition, a system according to some embodiments may be resistant to consumer-level attacks, which may include installation of circumvention devices or interface products. Connection of cables or devices outside the host device 24 does not result in compromise of the copy protection scheme implemented in the host device 24.

Another feature of a system according to some embodiments is that the conditional access system (in this case including the head-end system 14 and POD module 26) can restrict which host device a POD module can communicate with. The conditional access system is capable of identifying and disabling a suspicious host device, which is done in some embodiments by transmitting binding messages from the head-end system 14 only if the POD module 26 and the host device 24 have been verified by the head-end system 14

- 21 -

based on a comparison of values in one or more stored databases provided by a trusted third party.

The entity authentication and session key derivation process may be performed independent of the payload cipher algorithm, such as the conditional access algorithm. The authentication and key derivation process is relatively simple to implement in software executable on the host device 24 and POD module 26 with reduced involvement from hardware. In other embodiments, the authentication key derivation process may be implemented in hardware. In the CA-CP system according to some embodiments, the head-end system 14 is able to revoke authority of access to a host device in case of a break in the system. The copy protection scheme protects the exposed bus between the POD module and the host device and between the POD module and the head-end system.

Various software or firmware (formed of modules, routines, or other layers, for example), including applications and routines may be stored or otherwise tangibly embodied in one or more machine-readable storage media in the information transmission system. Storage media suitable for tangibly embodying software and firmware instructions may include different forms of memory including semiconductor memory devices such as dynamic or static random access memories, erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs), and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; and optical media such as CD or DVD disks. The instructions stored in the one or more storage media when executed cause the information transmission system to perform programmed acts.

The software or firmware can be loaded into the information transmission system in one of many different ways. For example, instructions or other code segments stored on one or more storage media or transported through a network interface card, modem, or other interface mechanism may be loaded into the information transmission system and executed to perform programmed acts. In the loading or transport process, data signals that are embodied as carrier waves (transmitted over telephone lines, network lines, wireless links, cables and the like) may communicate the instructions or code segments to the information transmission system.

While the invention has been disclosed with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations

- 22 -

therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of the invention.

- 23 -

What is claimed is:

- 1 1. A method of authenticating first and second devices, comprising:
2 receiving, in a third device, identifiers of the first and second devices;
3 retrieving information in the third device based on the identifiers;
4 transmitting, from the third device, a message based on the retrieved
5 information; and
6 verifying, in the first and second devices, identities of the other one of the first
7 and second devices based on the message.
- 1 2. The method of claim 1, wherein the transmitting includes transmitting a
2 message including public keys of the first and second devices.
- 1 3. The method of claim 2, wherein the transmitting includes transmitting a
2 message including reciprocals of the public keys of the first and second devices.
- 1 4. The method of claim 1, wherein the verifying includes performing
2 authentication using a public-key cryptographic protocol.
- 1 5. The method of claim 4, wherein the verifying includes performing
2 authentication using a discrete logarithmic version of a public-key cryptographic protocol.
- 1 6. The method of claim 5, wherein the verifying includes performing
2 authentication using an ElGamal cryptographic protocol.
- 1 7. The method of claim 1, further comprising generating a random number in the
2 first and second devices, wherein the verifying includes using the random number in each of
3 the first and second devices.
- 1 8. A method of securely communicating content between a first device and a
2 second device, comprising:
3 sending identification information of the first and second devices to a third
4 device;

- 24 -

5 generating, in the third device, a predetermined message based on the
6 identification information; and
7 authenticating the first and second devices using the predetermined message.

1 9. An apparatus for communicating with a first system, comprising:
2 a receiver including a first module and a second module coupled to the first
3 module, the first and second modules adapted to transmit identification information to the
4 first system and to authenticate each other based on predetermined information created and
5 sent by the first system in response to the identification information.

1 10. The apparatus of claim 8, wherein the first and second modules are adapted to
2 authenticate each other by using a public-key protocol.

1 11. The apparatus of claim 9, wherein the public-key protocol includes an
2 ElGamal protocol.

1 12. The apparatus of claim 9, wherein the receiver is adapted to receive content
2 from the first system that is protected by a first security protocol.

1 13. The apparatus of claim 12, wherein the first and second modules are adapted
2 to perform authentication according to a second security protocol including a discrete
3 logarithmic version of a public-key protocol.

1 14. A system comprising:
2 a conditional access system adapted to communicate content according to a
3 first security protocol;
4 a transport medium over which the content is communicated; and
5 a receiver coupled to the transport medium and including a first unit and a
6 second unit coupled by a communications channel, the first and second units adapted to
7 provide a second security protocol to protect information transmitted between the first and
8 second units, and

- 25 -

9 the conditional access system adapted to generate a predetermined message
10 and the first and second units adapted to authenticate each other based on the predetermined
11 message.

1 15. The system of claim 14, wherein the receiver includes a content protection
2 system.

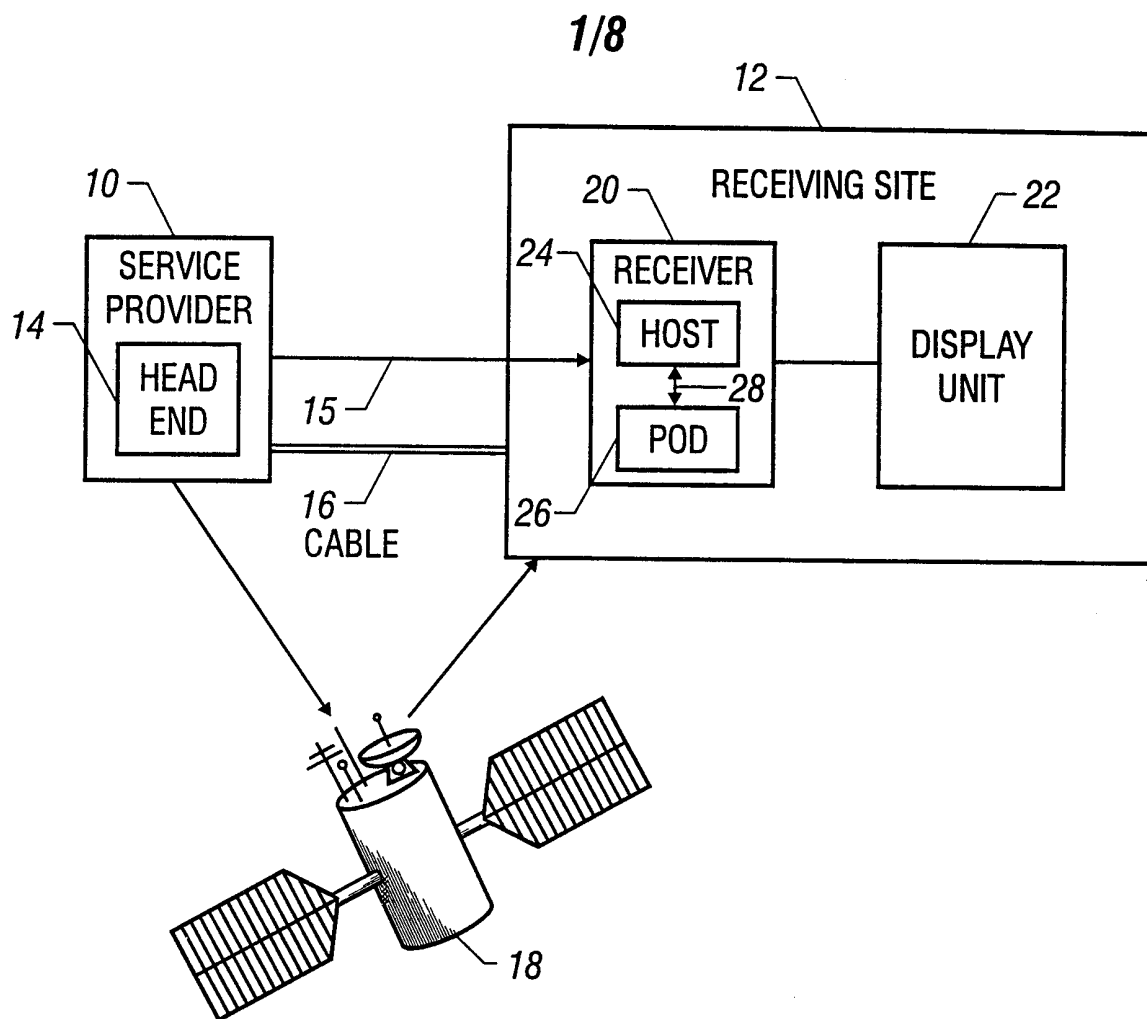
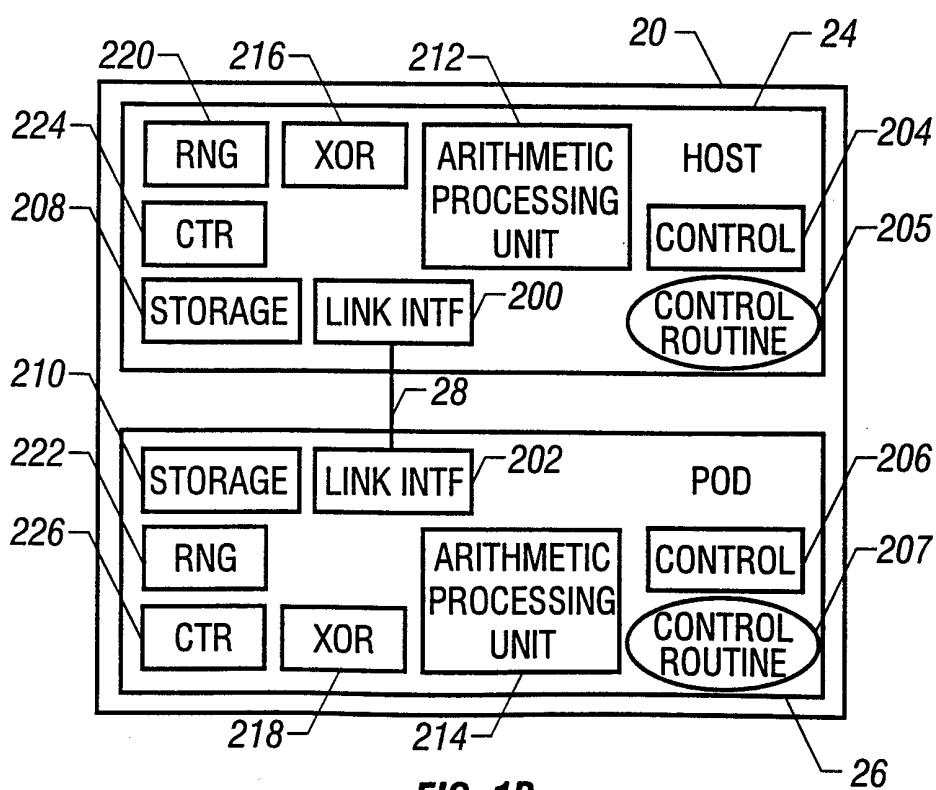
1 16. The system of claim 15, wherein the conditional access system includes a
2 transmission head-end and the first unit of the receiver.

1 17. The system of claim 14, wherein the first and second units are adapted to
2 generate a session key based on the predetermined message to protect information transmitted
3 over the communications channel.

1 18. The system of claim 14, wherein the conditional access system includes a
2 transmission head-end adapted to encrypt video content to transmit over the transport
3 medium.

1 19. The system of claim 14, wherein the first and second units are adapted to
2 authenticate each other according to a discrete logarithmic version of a public-key
3 cryptographic protocol.

1 20. An article including one or more machine-readable storage media containing
2 instructions to protect communications between first and second devices in a system, the
3 instructions when executed causing the system to:
4 transmit identifiers of the first and second devices to an external system;
5 receive a predetermined message from the external system that is based on the
6 identifiers; and
7 authenticate the first and second devices based on the predetermined message.

**FIG. 1A****FIG. 1B**

2/8

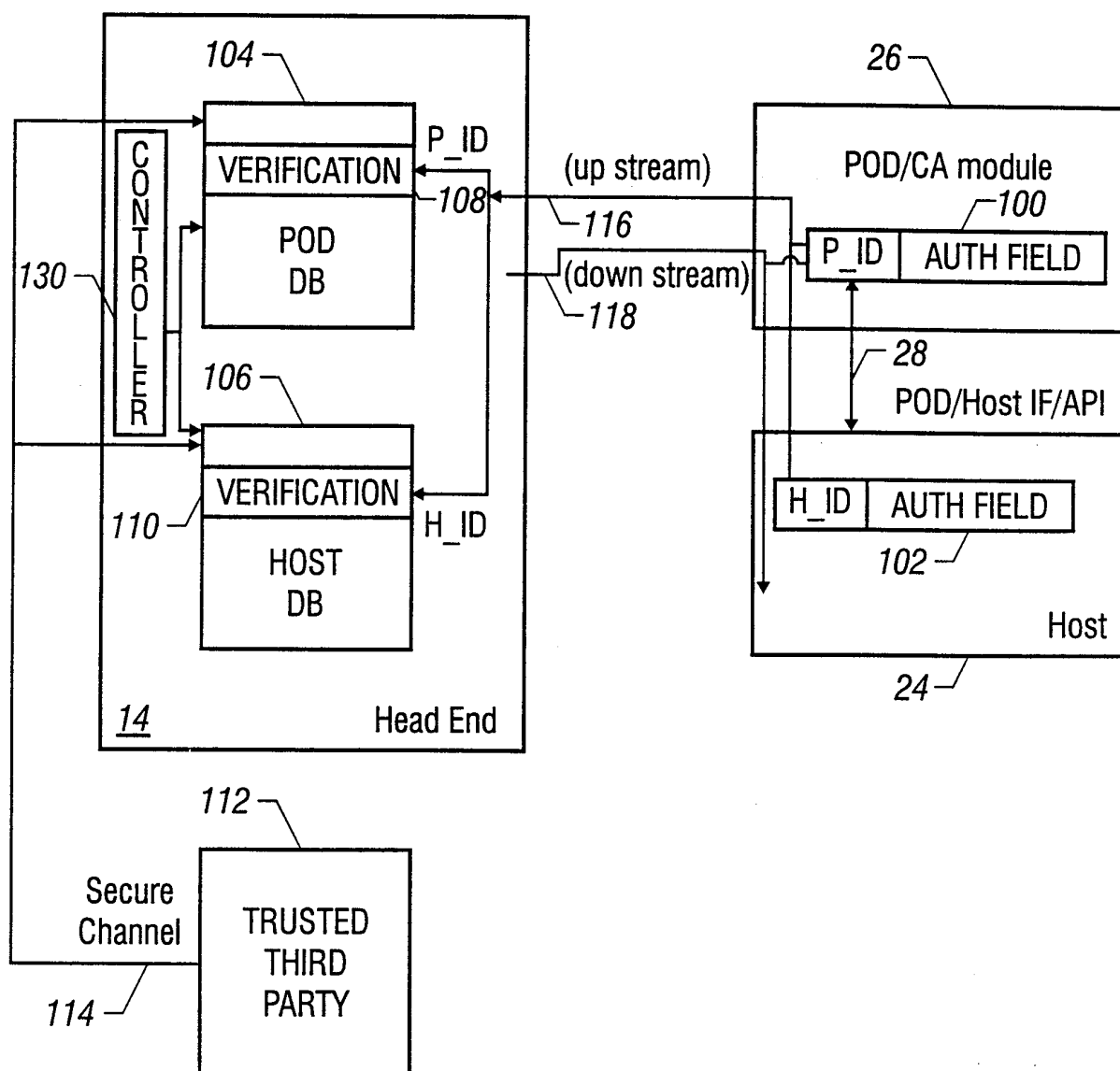


FIG. 2

3/8

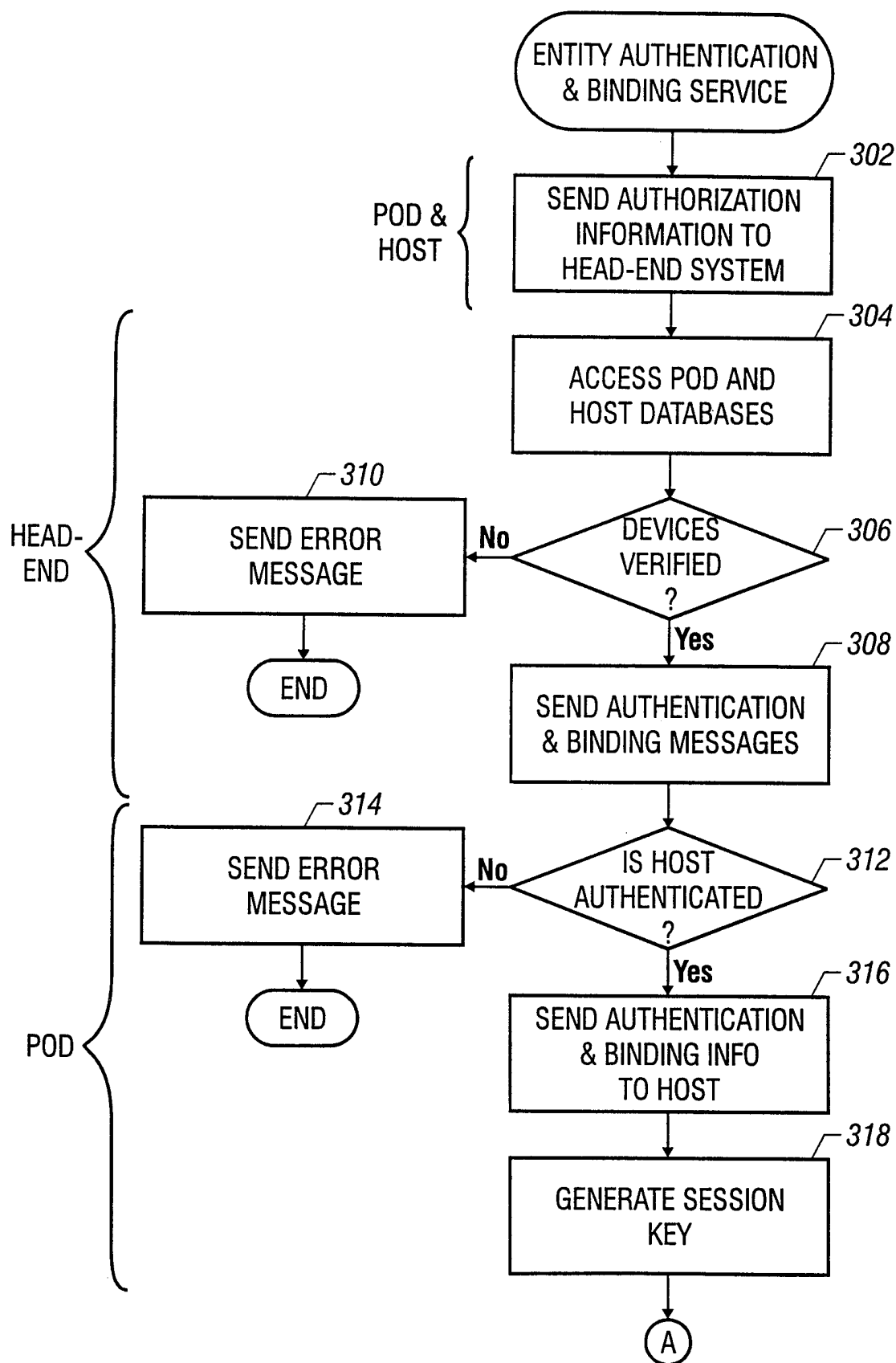
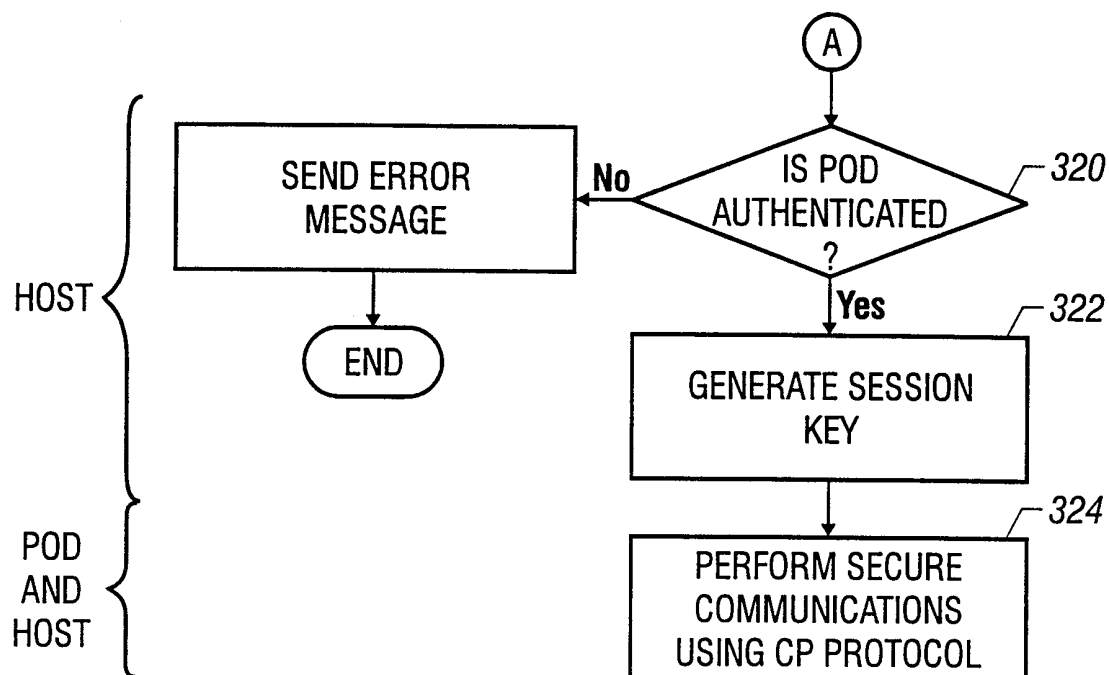


FIG. 3A

4/8

**FIG. 3B**

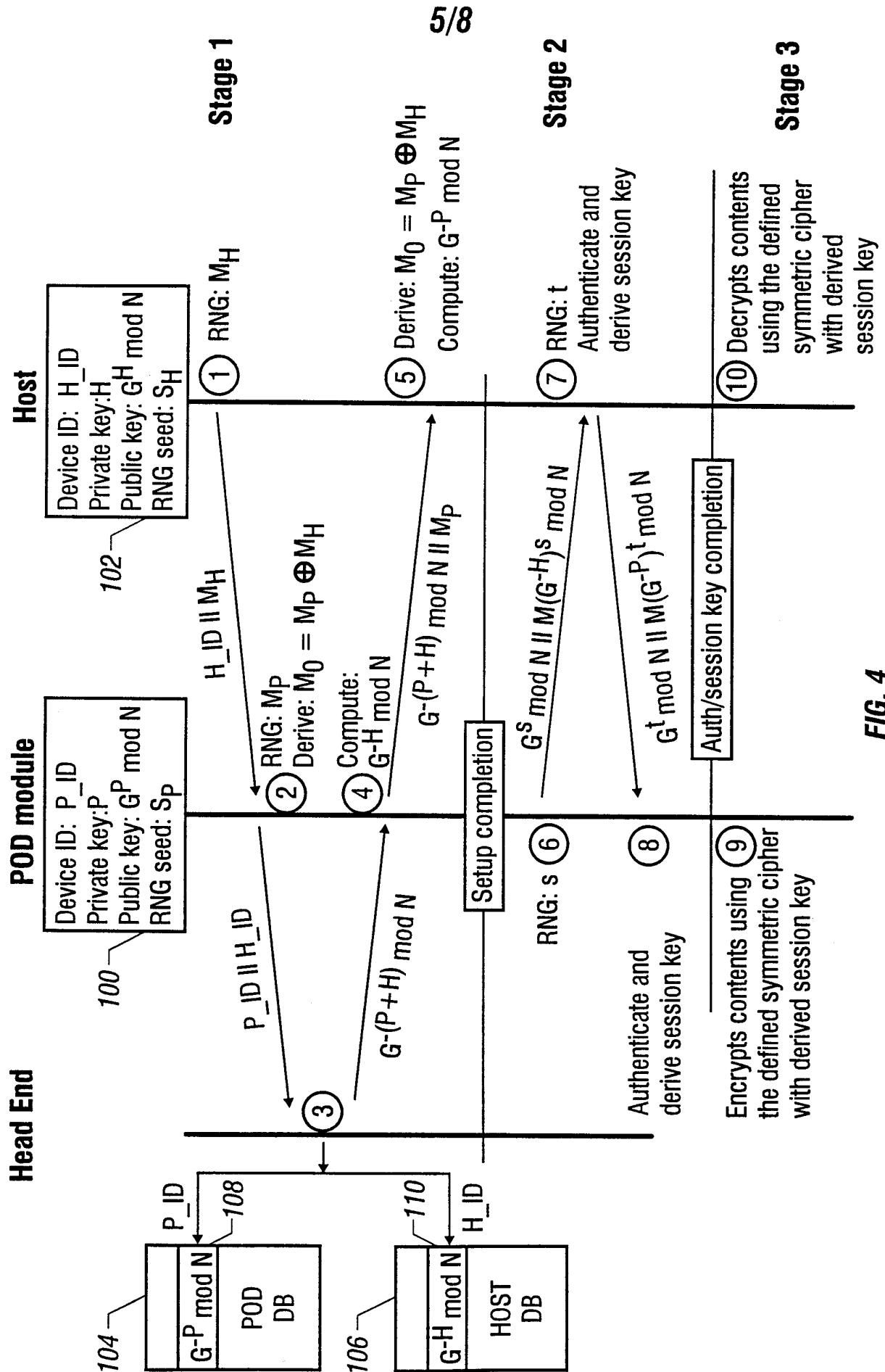


FIG. 4

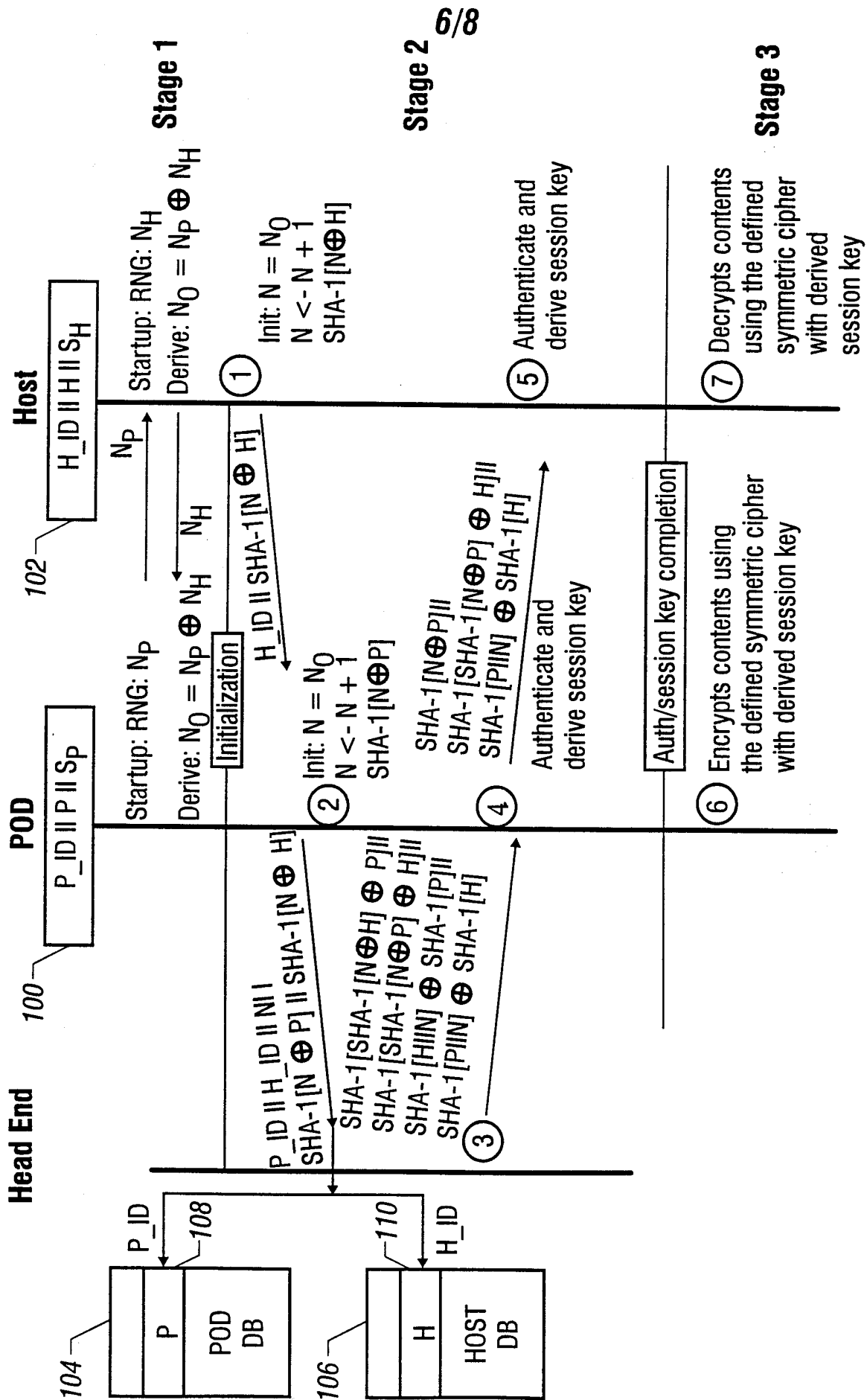


FIG. 5

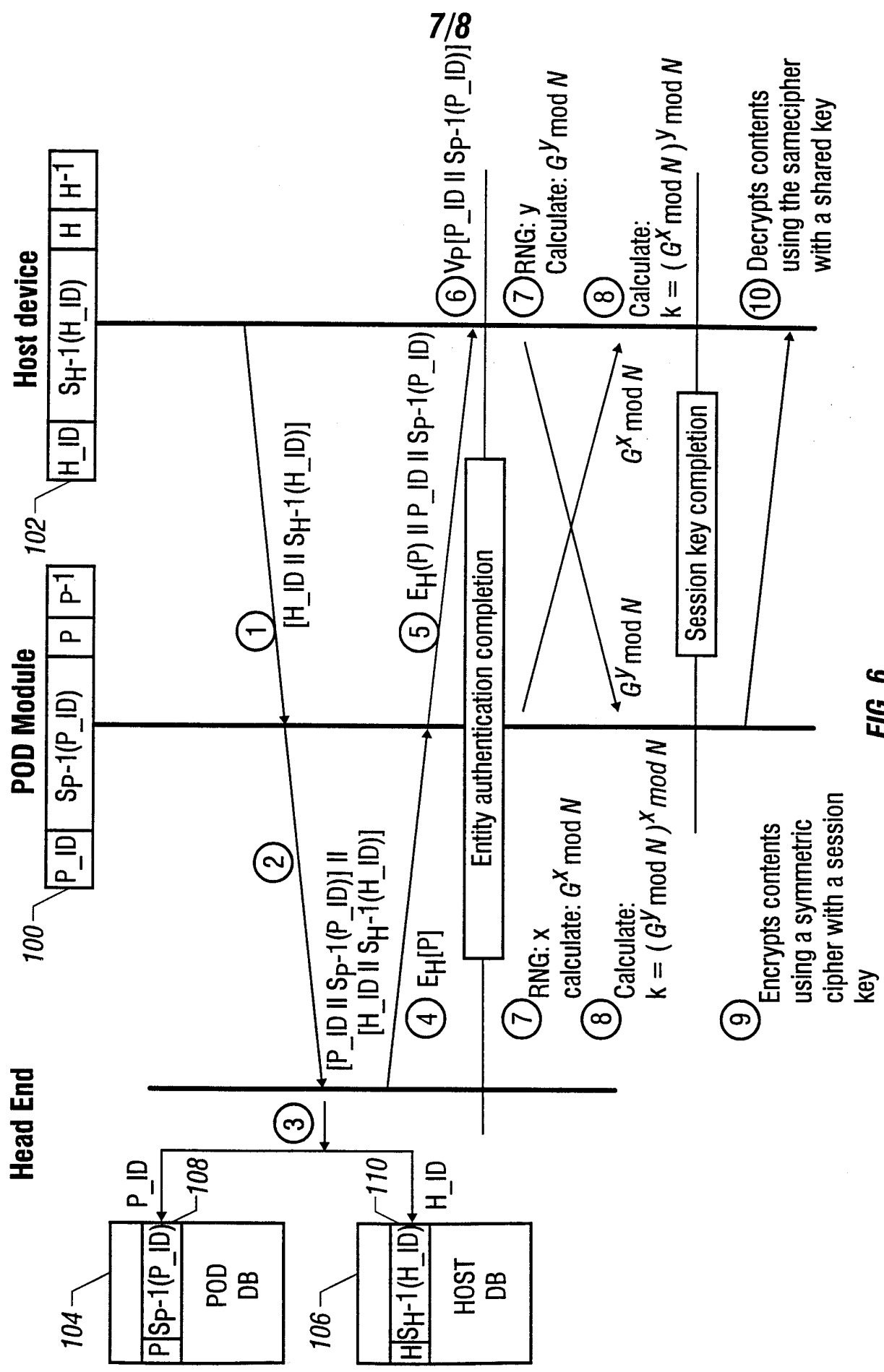
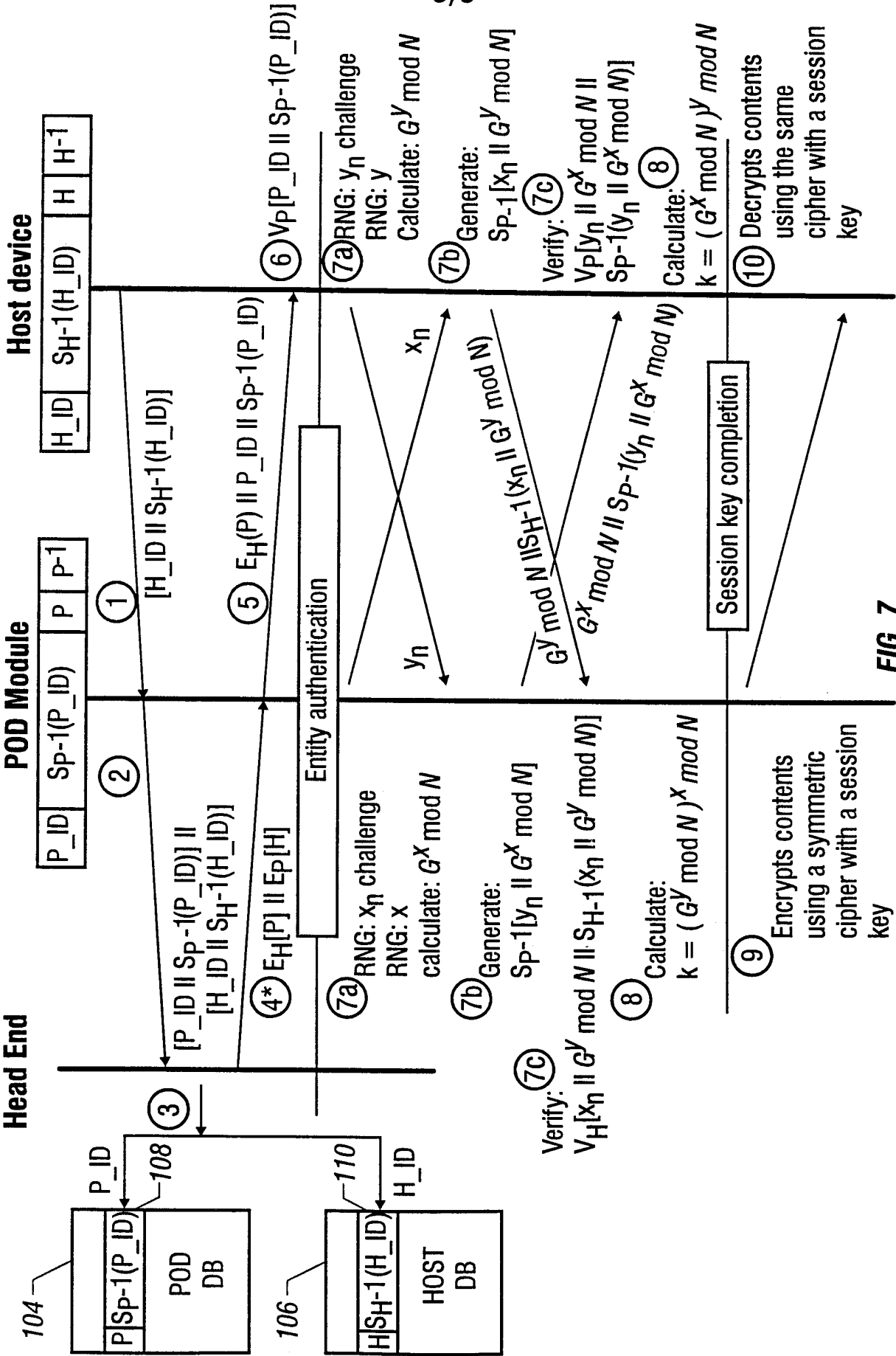


FIG. 6



INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 00/00713

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/32 H04N7/16

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L H04N

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SCHNEIER: "APPLIED CRYPTOGRAPHY" 1996, WILEY & SONS, NEW YORK XP002138607 page 56, line 28 - line 34 page 63, line 1 - line 16 ----	1,8-10, 20
A	WO 97 38530 A (DAVIES DONALD WATTS ;GLASSPOOL ANDREW (GB); DIGCO B V (NL); RIX SI) 16 October 1997 (1997-10-16) page 1, line 13 -page 2, line 13 page 4, line 1 -page 5, line 17 ----	8,14
A	WO 98 56179 A (ESKICIOGLU AHMET MURSIT ;VIRAG DAVID EMERY (US); WEHMEYER KEITH RE) 10 December 1998 (1998-12-10) page 6, line 1 -page 12, line 13 -----	8,14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents:

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

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

24 May 2000

Date of mailing of the international search report

09/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/US 00/00713

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9738530 A	16-10-1997	AU 2506397 A BR 9708500 A CA 2250833 A CN 1215528 A EP 0891670 A HR 970160 A	29-10-1997 03-08-1999 16-10-1997 28-04-1999 20-01-1999 28-02-1998
WO 9856179 A	10-12-1998	AU 7725898 A EP 0986910 A	21-12-1998 22-03-2000