(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2001/0019613 A1**
Dillon et al. (43) **Pub. Date: Sep. 6, 2001**

(54) **ADAPTER FOR CONNECTING COMPUTER TO SATELLITE ANTENNA**

(75) Inventors: **Douglas M. Dillon**, Gaithersburg, MD (US); **Robert D. Cassagnol**, Silver Spring, MD (US)

Correspondence Address:
HUGHES ELECTRONICS CORPORATION
PATENT DOCKET ADMINISTRATION
BLDG 001 M/S A109
P O BOX 956
EL SEGUNDO, CA 902450956

(73) Assignee: **HUGHES ELECTRONICS**

(57) **ABSTRACT**

A method and apparatus for an adapter card, for use in a computer, to provide conditional access by the computer to incoming data streams while maintaining the security of information by maintaining a listing of addresses corresponding to data streams which the computer is authorized to receive, receiving and determining the address of a frame, determining whether the frame address matches an address maintained in an Access Table, and processing and transmitting only those frames of data streams which the computer is authorized to receive.
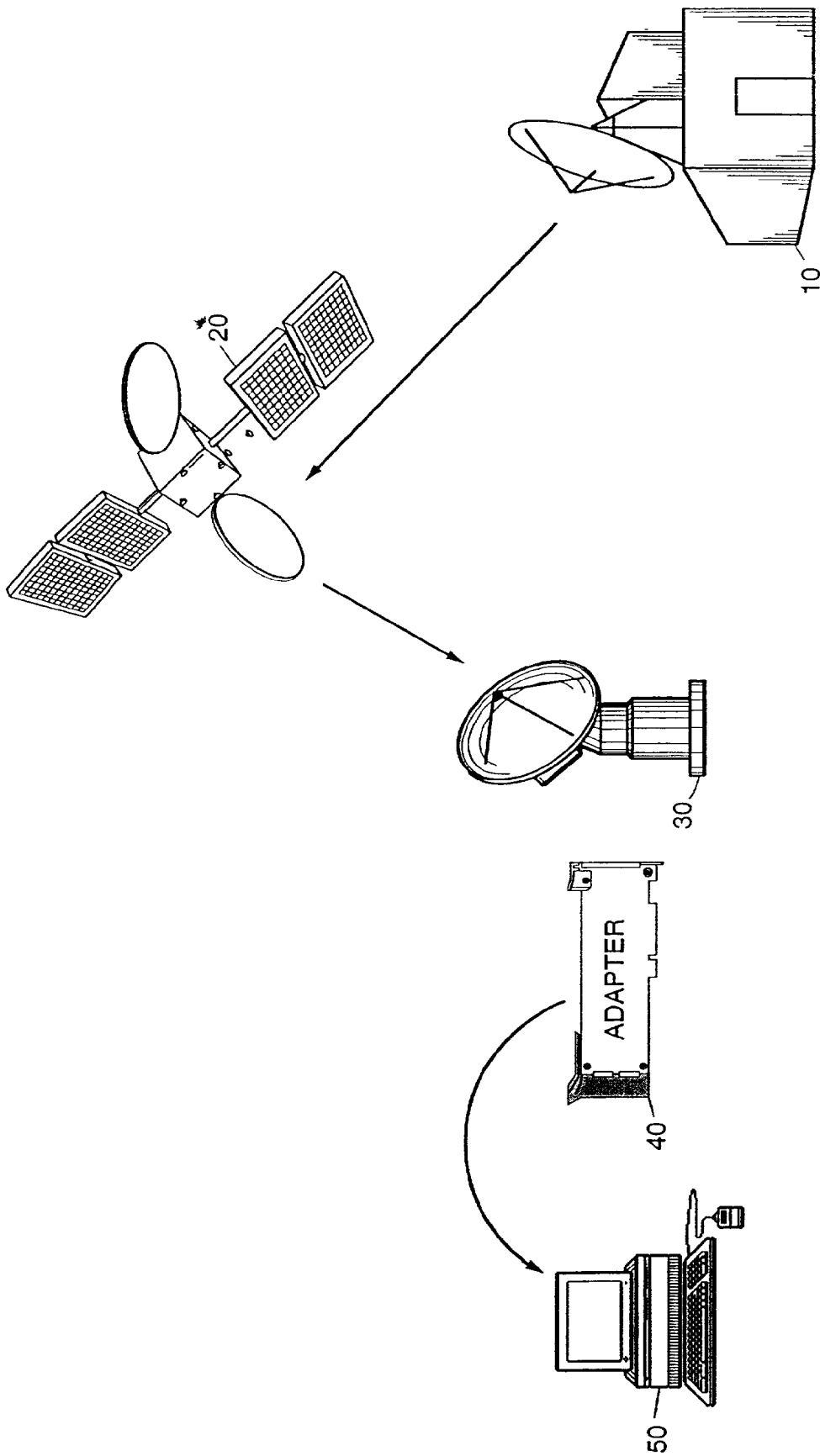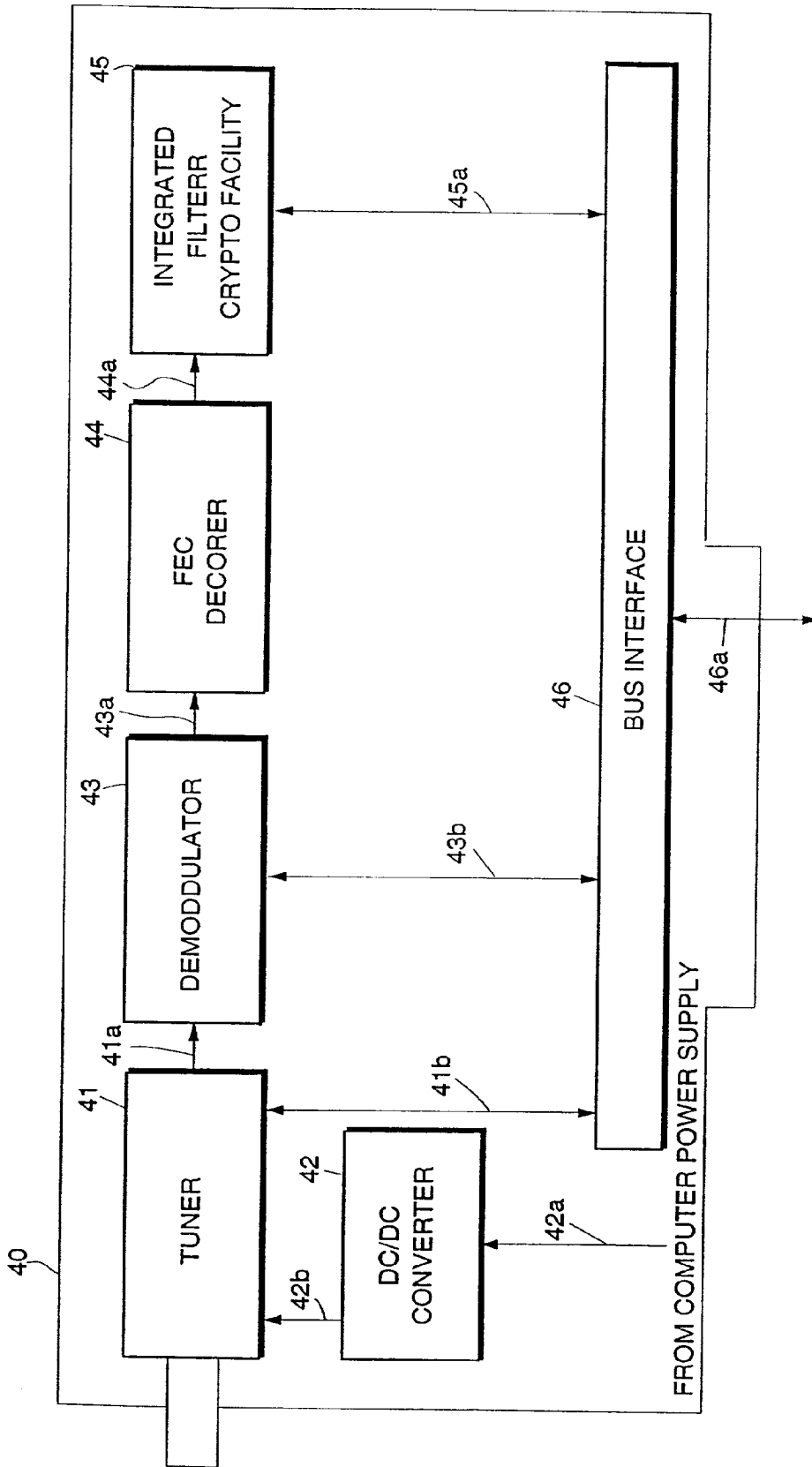
10

20

30

40

ADAPTER

50
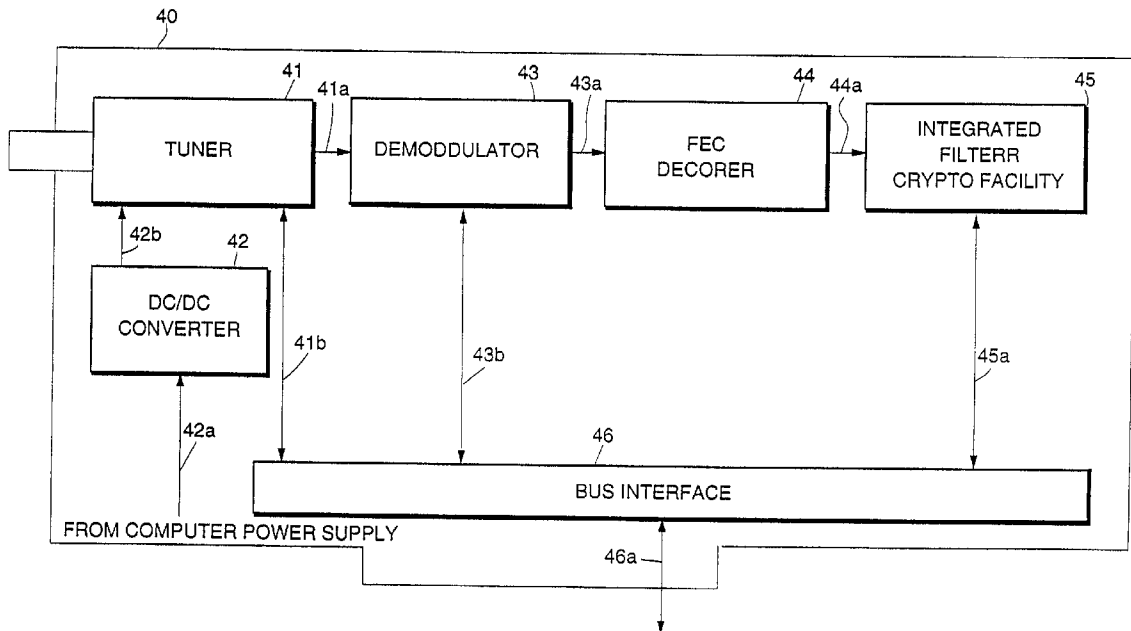
FIG. 1.

FIG. 2.

ADAPTER FOR CONNECTING COMPUTER TO SATELLITE ANTENNA

RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of copending application Ser. No. 08/340,347, entitled "Apparatus and Method for Satellite Receiver Computer Adaptor Card," filed on Nov. 14, 1994.

FIELD OF THE INVENTION

[0002] The present invention relates generally to the field of communications, and more specifically to conditional access by computers to data streams transmitted via satellite.

BACKGROUND OF THE INVENTION

[0003] Satellite communication has long been used to broadcast data to computers. In situations requiring the same data to be transmitted to multiple sites, satellite communication, which allows a single transmission of data to be received at multiple sites, can be more cost effective than terrestrial communication, which requires separate transmission to each site.

[0004] In the past, data broadcast via satellite to a computer typically was received by an external satellite receiver, which serially passed a single data stream to the computer through a serial adapter interface. An example of such a system is the Opportunistic Data File Broadcast system developed by Hughes Network Systems, which employs a Compression Labs Spectrum Saver satellite receiver to pass RS-422 serial data to high-speed adapters in computers at remote sites. This particular system has been used by financial institutions to broadcast financial data from central data centers to branch offices.

[0005] For commercial data broadcasts, conditional access technology enabling only authorized users to access the broadcast data is essential to ensure payment for the data. Conditional access is typically implemented by encrypting the broadcast data and providing the decryption keys only to authorized receivers. In prior satellite data communication systems, such as the Opportunistic Data File Broadcast system, conditional access functions have been performed by the external satellite receiver, which outputs a single decrypted data stream to the receiving computer. In these systems, conditional access is provided for only a single data stream. Thus, to access multiple data streams simultaneously transmitted would require users to have a complete set of receiving equipment for each data stream.

[0006] Another type of satellite communication system has been suggested in which an adapter card, insertable into a computer, enables satellite reception without the need for the external satellite receiver. Examples of such systems are disclosed in U.S. Pat. No. 4,777,657 to Gillaspie, U.S. Pat. No. 5,019,910 to Filmer, and U.S. Pat. No. 5,359,367 to Stockill.

[0007] However, these references fail to teach a system incorporating conditional access technology, and similarly fail to provide for simultaneous receipt of multiple data streams where the data streams are individually conditional access controlled. Furthermore, to the extent that the prior art discloses use of decryption hardware, none of the prior art systems extends the use of the hardware beyond decrypting an incoming broadcast data stream to providing encryption and decryption operations for the connected computer.

SUMMARY OF THE INVENTION

[0008] The present invention addresses the shortcomings of prior art systems by teaching a secure satellite communication system for providing subscribers with conditional access to broadcast satellite data through their computers. This system maintains the security of information by providing access only to authorized users, and provides an additional benefit by enabling users to concurrently receive and decrypt multiple data streams.

[0009] In a preferred embodiment, the present invention teaches a method for an adapter card, for use in a computer, to provide conditional access by the computer to input data, including data streams transmitted via satellite, wherein a data stream is comprised of at least one frame and each frame includes an address identifying the data stream. This method includes the steps of maintaining an Access Table, in which each table entry includes an address field for storing an address corresponding to a data stream which the computer is authorized to receive, receiving a frame and determining its address, and determining whether the frame address matches an address maintained in the Access Table in order to determine whether the computer has access to the data stream corresponding to the frame. If a match is not found, the adapter card discards the frame, but if a match is found, the adapter card processes and transmits the frame to the computer through a bus interface.

[0010] In a preferred embodiment, the adapter card additionally is capable of processing data transmitted from the computer.

[0011] In addition to the method described above, the present invention is also directed to an adapter card for use in a computer, for providing conditional access by the computer to input data including frames of data streams transmitted via satellite, wherein each data stream is comprised of at least one frame and each frame includes an address identifying the data stream. The adapter card includes a receiver for receiving a data stream frame, an Access Table, in which each table entry includes an address field for storing an address corresponding to a data stream which the computer is authorized to receive, an integrated filter/crypto (IFC) block for determining an address of the received frame and determining whether the frame address matches an address maintained in the Access Table, and a bus interface for enabling communication between the adapter card and the computer. If the IFC finds that the frame address does not match a table address, the IFC block discards the frame, but if it finds a match, the IFC block processes the frame into output data, to be transmitted to the computer via the bus interface. The IFC preferably is also capable of processing data input from the computer into output data.

[0012] The invention itself, together with further objects and attendant advantages, will best be understood by reference to the following detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is an illustration of one form of satellite broadcast system in which the present invention may be implemented.

[0014]   FIG. 2 is a block diagram of the preferred embodiment of the adapter card receiver of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015]   It is envisioned that the present invention will be used in conjunction with a satellite broadcast system such as that shown in **FIG. 1**. As illustrated, this system includes a network operations center (NOC) **10**, satellites **20**, antenna receivers **30**, adapter card receivers **40** (adapter cards), and computers **50**.

[0016]   In this system, a subscriber, through an adapter card **40** inserted in a computer **50**, receives information in data streams broadcast via satellite **20**. The data streams are uplinked to one or more communications satellites **20** by the NOC **10** from a large antenna broadcast earth station. Each data stream is broadcast in units of frames, with each frame including an address header for identifying the data stream, a data field containing data, and a CRC tail for ensuring accurate transmission. Preferably, the frames are encrypted, and the key needed to decrypt the data of a frame is identified by its address header. Accordingly, data can be accessed only by receivers having the proper key.

[0017]   Each antenna receiver **30**, comprising a smaller antenna and low-noise block (LNB) element, receives the broadcast frames and transmits the frames to a connected adapter card **40** inserted in the subscriber's computer **50**. Because the subscriber may have access to only a subset of the broadcast data streams, the adapter card **40** screens incoming frames, and processes only those frames the subscriber is authorized to receive by using the frame address field to retrieve the corresponding key for decrypting each frame. The adapter card **40** then transmits the decrypted frames through a bus interface to the computer **50**.

[0018]   The present invention is directed to the adapter card **40**, which provides the conditional access to incoming data streams, and preferably enables concurrent reception of multiple data streams. By processing only authorized frames and discarding all others, the present invention prevents unauthorized frames from ever being passed to the computer **50**. This not only prevents subscribers from illicitly accessing the decrypted data stream, but also provides a physical measure of security by preventing the encrypted data stream from being made available to be downloaded into the computer **50**. This is an important feature because security mechanisms have been evaded by downloading encrypted data, as once the encrypted data stream is stored in the computer memory, the user can access the data for as many attempts as needed for decryption.

[0019]   By evaluating and decrypting incoming data streams on a frame-by-frame basis, the present invention enables simultaneous reception of multiple conditional access controlled data streams statistically multiplexed in a received signal. Furthermore, because the present invention further enables frames to be decrypted as they are received, the need for buffer RAMs required in prior systems to store incoming frames can be substantially reduced or eliminated, thereby lowering the cost of the systems.

[0020]   As explained in greater detail below, the preferred embodiment of the present invention increases the security of the conditional access provided to the transmitted data

streams by providing a secure management system for the decryption keys. More specifically, the preferred embodiment provides a system having at least two levels of encryption, in which the decryption keys are themselves encrypted and never appear to users in decrypted or human-intelligible form.

[0021]   In the preferred embodiment, the adapter card **40** additionally provides the encrypting and decrypting capabilities of the adapter card **40** to be used by the computer **50** as a general purpose bulk data encryptor/decryptor, even while the adapter card **40** is concurrently processing received frames. Not only does this feature reduce the overall cost to the user by eliminating the need for a separate data encryption/decryption engine to handle computer data, it also permits the advantageous conditional access features of the present invention to be provided to data received by the adapter card **40** from the computer **50** via a number of possible sources, rather than from the satellite **20** alone.

[0022]   **FIG. 2** illustrates the adapter card **40** of the preferred embodiment, which includes the following functional blocks:

   [0023]   1. Front End Block **41**, **42**: connects the adapter card receiver **40** to the antenna receiver **30**, for receiving a plurality of signals from the NOC **10** via the satellite **20** and transmitting data streams **41***a* from a particular signal selected by the tuner **41** to the Demodulator Block **43**;

   [0024]   2. Demodulator Block **43**: converts data streams **41***a* received on the selected signal into digital form and transmits the demodulated data stream **43***a* to the FEC Decoder Block **44**;

   [0025]   3. FEC Decoder Block **44**: identifies and corrects transmission errors in the demodulated data stream **43***a* and transmits the corrected data stream **44***a* to the Integrated Filter/Crypto Block **45**;

   [0026]   4. Integrated Filter/Crypto Block **45**: identifies frames within the received data stream **44***a* and decrypts frames of the accessible data streams; and

   [0027]   5. Bus Interface Block **46**: enables communication between the adapter card **40** and the computer **50**.

[0028]   1. Front End Block

[0029]   In the preferred embodiment, as illustrated in **FIG. 2**, the Front End Block includes a tuner **41**, which can be set to receive an IF signal in 100 kHz steps in the frequency range of 950 to 1450 MHz, and downconverts the received signal to an IF output centered at 60 MHz. The operation of the tuner **41** can be controlled **41***b* by the computer **50** through the Bus Interface Block **46**, or in a preferred embodiment, a local microprocessor may be provided on the adapter card **40** to monitor and control the tuner **41**.

[0030]   The Front End Block preferably also comprises a DC-DC converter **42**, to provide all power required by the tuner **41** as well as the attached LNB by converting a +5V signal **42***a* received from the computer power supply to voltages required by the various components (e.g., **42***b*).

[0031] 2. Demodulator Block

[0032] The Demodulator Block **43** receives and demodulates the downconverted signal **41***a* from the Front End Block. In the preferred embodiment, the Demodulator Block **43** is implemented in a CMOS ASIC, and, through control **43***b* by the computer **50** or an adapter card microprocessor, provides all baseband signal processing required for demodulation.

[0033] 3. FEC Decoder Block

[0034] The FEC Decoder Block **44** uses redundant data in the demodulated digital data stream **43***a* to identify and correct transmission errors. In the preferred embodiment, FEC Decoder Block **44** consists of a Viterbi soft-decision decoder, depuncture logic which allows the rate ½ Viterbi to operate at an effective rate of ⅔, a deinterleaver which scatters the errors resulting from the incorrect attempts to correct data, and a Reed-Solomon decoder capable of correcting the scattered errors.

[0035] 4. Integrated Filter and Crypto Facility Block

[0036] The Integrated Filter and Crypto Facility (IFC) Block **45** plays a primary role in enabling the inventive conditional access features provided.

[0037] The IFC **45** receives frames of the digital data streams **44***a,* which are preferably encrypted. In the preferred embodiment, the standard DES algorithm is used, although alternative encryption algorithms are possible as well.

[0038] There are numerous methods by which users can acquire decryption keys, and the present invention can be adapted for use with any of these methods. For example, a subscriber can obtain a "smart card" from the service provider, typically a credit-card sized card readable by the computer. In some cases, the information provider can send information that passes into the smart card to generate the decryption keys. Another method is to obtain the keys through messages received from the satellite link or over a terrestrial communications system (e.g., via a modem connected to the computer). Still another method is for the subscriber to obtain the keys orally from the information provider and to manually enter the keys into the computer through the keyboard input.

[0039] The security of the present invention can be maintained with any of these systems because it does not depend solely on the security of the actual transmission of the keys. Rather, the security system of the present invention has multiple levels of security. At a first level, to receive any satellite data stream, a user must subscribe to the service provider and must obtain the necessary wiring and equipment. At the next level, security is enhanced by means of "groups." Each group comprises a set of data streams, and a subscriber must have access to a particular group in order to receive any of its data streams. Finally, in the preferred embodiment, an additional level may be provided by requiring subscribers to have specific authorization to receive each individual data stream within a group.

[0040] The present invention implements this tiered conditional access system through key management. Users become subscribers by subscribing to the service provider and obtaining an adapter card receiver **40**, having an IFC **45**, to be inserted into a computer **50**. In the preferred embodi-

ment, the IFC **45** is physically secured by implementation in an ASIC, which is equipped with a burned-in Master Key used for identification purposes. In the preferred embodiment, a unique Master Key is used for each IFC **45**.

[0041] Preferably, to enhance the security of the conditional access features provided, the Master Key is used for subscriber identification rather than decryption. Accordingly, each adapter card **40** is also assigned a unique User Key which is encrypted with the Master Key before being distributed to the subscriber, and is decrypted only within the IFC **45**. This prevents the User Key from ever appearing in unencrypted form, even to the subscriber. Use of the User Key rather than the Master Key allows the Master Key to be kept physically secure within the ASIC and minimizes its use, thereby minimizing its exposure. Consequently, the only method of compromising the security of the Master Key is by breaking the algorithm used to encrypt the User Key or by compromising the physical security of the IFC **45**. Furthermore, the security of the overall system can be maintained through key distribution by simply changing a subscriber's User Key. This avoids the need for physical replacement of the IFC **45** even if the security of the User Key is compromised.

[0042] In the preferred embodiment having group access requirements, the function of the User Key is to decrypt Group Keys. A subscriber wanting to access any data stream within a particular group must have the Group Key for that group. A Group Key can be distributed to subscribers by any appropriate means with little risk to the security of the system because the entity providing distribution of Group Keys will encrypt a Group Key with the subscriber's unique User Key before transmission. Accordingly, the Group Key can be decrypted only by the IFC **45** of the subscriber for which it is intended, minimizing the likelihood that it will be distributed to and successfully used by an unauthorized user. Furthermore, even the authorized subscriber will never have access to the decrypted Group Key, because the Group Key is encrypted by the User Key until decrypted within the physically secure IFC ASIC, and as described above, the subscriber does not have access to the User Key.

[0043] In the preferred embodiment, the only function of a Group Key is to decrypt Data Keys for the data streams within the group. As discussed, because a subscriber must be a member of a group to access any of the data streams within the group, only subscribers having the appropriate Group Key can decrypt the Data Key. Additionally, because each Data Key is encrypted with its Group Key before being distributed to subscribers, in order to access and decrypt a particular data stream within a group, the subscriber must have the appropriate Data Key for that data stream.

[0044] The combination of the Group Keys and the Data Keys determine the subscriber's accessibility to the incoming data streams, and must be kept current. In the preferred embodiment, an Access Table is stored in adapter card memory outside of the IFC **45**, with entries corresponding to data streams the subscriber is authorized to receive. Each entry accordingly has fields for an address of a data stream the subscriber is authorized to access, and a Group Key and a Data Key required to decrypt that data stream. Because this table is located outside the IFC **45**, the Group and Data Keys are stored in encrypted form in the Access Table. A microprocessor is preferably provided on the adapter card **40**

outside the IFC **45** to perform the table functions and to indicate to the IFC **45** whether a particular address matches a table entry, and also to indicate the appropriate key, if a match is found.

[0045] In the preferred embodiment, other aspects of the key management system are implemented within the IFC ASIC. For example, logic is provided for maintaining and storing current keys, as well as for handling data in both encrypted and decrypted form. As earlier noted, the IFC **45** in a preferred embodiment provides decryption functions for incoming frames as well as encryption and decryption functions for bulk data from the computer **50**. To provide these features, the ASIC logic includes at least the following subblocks:

[0046] UK Register, for storing the User Key of the subscriber, which as described above, is decrypted by the Master Key as it is loaded into the IFC **45**;

[0047] GK Register, for storing a single Group Key. Although a subscriber may have access to more than one group, as described above, the preferred embodiment provides an access table outside the IFC **45** for storing the Group Keys in encrypted form. When the IFC **45** receives an encrypted frame, it extracts the data stream address, and if the address matches one of the access table entries, the appropriate Group Key is decrypted by the User Key as it is loaded into the IFC **45**;

[0048] DK Register, for storing a Data Key to decrypt input data, whether satellite data or computer data;

[0049] an encryption/decryption engine, for performing the actual decryption of satellite data, or encryption or decryption of computer data from other sources;

[0050] Input Registers, for storing input yet to be processed, preferably including at least one register specifically designated for satellite data and at least one register specifically designated for computer data;

[0051] Opcode Registers, for indicating the location of the appropriate key for a particular operation and the location where the output should be stored, preferably including at least one register specifically designated for satellite data and at least one register specifically designated for computer data; and

[0052] Output Registers, preferably including at least one register specifically designated for satellite data and at least one register specifically designated for computer data from other sources.

[0053] In the preferred embodiment, the logic is implemented to provide functions for loading Group Keys, loading Data Keys, processing satellite data, and processing computer data. The Load Group Key function is used to provide the IFC **45** with the necessary Group Key for decryption, when the address of a received frame matches an address stored in the access table. Input to the Load Group Key function is a Group Key encrypted by the User Key. When the IFC **45** receives this instruction, it retrieves the User Key from the UK Register to decrypt the received Group Key, and stores the decrypted Group Key in the GK Register.

[0054] A Load Data Key instruction indicates to the IFC **45** that the input is a Data Key encrypted by a Group Key. In response, the IFC **45** will decrypt the input with the Group Key stored in the GK Register and store the resulting decrypted Data Key in the DK Register.

[0055] When the IFC **45** receives a Process Satellite Data instruction, the input contains an incoming satellite data stream frame. The IFC **45** locates the address in the address header of the frame and determines whether it has the Data Key necessary for decryption by searching the access table for the frame address. If a match is found, the IFC **45** will retrieve the appropriate Group and Data Keys, decrypt the frame and store the decrypted frame in an Output Buffer for satellite data; if not, the IFC **45** will discard the frame.

[0056] Process Computer Data instructions are handled similarly. As previously noted, in the preferred embodiment, the IFC encryption/decryption engine is capable of encrypting and decrypting data from other sources, transmitted by the computer **50**. To enable operations to be simultaneously performed on both incoming satellite frames as well as incoming computer data, the IFC **45** time shares between frame reception and data encryption and decryption operations. To process computer data, the computer **50** must transmit the key to be used, an indication of whether the key is to be used for encryption or decryption, and the data on which the operation is to be performed. Based on this input, the IFC **45** will perform the appropriate operation on the data and return the processed data to the attached computer **50** via the Bus Interface Block **46**.

[0057] Thus, unlike systems described in prior art which simply transmit incoming data streams into the computer **50**, the IFC **45** of the present invention allows the computer **50** only conditional access to received data streams. In particular, only authorized signals are ever downloaded into the computer **50**. The preferred embodiment provides enhanced security by ensuring that none of the keys required at any level of decryption ever appears outside the IFC ASIC in decrypted form, and by providing multiple layers of security. These layers not only make unauthorized access more difficult, but by implementing the layers in the key management system, they also enable a fast, simple method to recover from most security problems. More specifically, in response to problems due to an unauthorized user obtaining a User Key assigned to an authorized subscriber, a new User Key can be distributed to that subscriber. Similarly, in response to security problems caused by unauthorized access to particular data streams, the data stream and group keys required for decrypting those data streams can be changed, and the updated keys provided only to authorized users.

[0058] Besides security, the IFC **45** provides data management benefits by efficiently using memory and computer processing time, which is especially useful in downloading large files. The present invention filters incoming data stream frames by determining whether the computer is authorized to receive the frame based on its address, accepting only authorized frames. This significantly reduces the adapter memory requirements, since individual frames are decrypted as they are received rather than requiring encrypted frames to be buffered in their entirety awaiting decryption. This feature may eliminate the need for buffer-

ing frames on the adapter entirely, eliminating the need for buffers on the adapter card **40** and providing a significant cost reduction.

[0059] Yet another advantage provided by the IFC **45** of the present invention is that, by providing address-based frame decryption, the adapter card **40** can simultaneously decrypt multiple data streams that are statistically multiplexed on the same broadcast signal.

[0060] One skilled in the art will recognize that variations for providing the required capabilities of the IFC **45**. For example, although the preferred embodiment is implemented with the three level security scheme described above, the present invention may be implemented with only two levels of security by providing only the User Keys and the Data Keys. In this case, the User Key serves the same purpose as in the three-level scheme, but the Data Keys will be provided to the adapter card **40** encrypted in the User Key rather than in a Group Key. Other levels of security may likewise be used without departing form the claimed invention.

[0061] 5. Bus Interface Block

[0062] The Bus Interface Block **46** enables communication **46a** between the computer and the adapter card **40** for, among other things, controlling and monitoring the tuner **41** and the demodulator **43** and maintaining the key management system. Additionally, the Bus Interface Block **46** allows the attached computer **50** to obtain decrypted frames from the IFC Block **46**, and to pass bulk data to the IFC **46** for encryption or decryption and receive the resulting processed data. After performing the required operation on incoming data, one implementation buffers the resulting data in memory provided on the adapter card **40**, and interrupts the attached computer **50** for retrieval. Alternatively, in a preferred embodiment, the Bus Interface Block **46** automatically reads the decrypted data into the memory of the attached computer **50**.

[0063] The present invention, as illustratively embodied in the preferred embodiment described above, provides an adapter card receiver **40**, to be used in conjunction with a connected computer **50**, for enabling users to conditionally access and quickly download multiple data streams, such as signals transmitted via satellite **20**. The invention also maintains the security of privileged information by preventing the information to enter the computer of unauthorized users.

[0064] However, it should be understood that a wide range of changes and modifications can be made to the preferred embodiment described above. It is therefore intended that the foregoing detailed description be illustrative rather than limiting, and that it is the following claims, including all equivalents, which are intended to define the scope of this invention.

What is claimed is:

1. A method for an adapter card, for use in a computer, to provide conditional access by the computer to input data streams, wherein a data stream is comprised of at least one frame and each frame includes an address identifying the data stream, comprising the steps of:

    maintaining an Access Table, wherein each table entry includes an address field for storing an address corresponding to a data stream which the computer is authorized to receive;

    receiving a frame;

    determining the address from the frame;

    determining whether the frame address matches an address maintained in the Access Table;

    discarding the frame if a match is not found; and

    processing and transmitting the frame to the computer through a bus interface if a match is found.

2. The method of claim 1, wherein the data streams are transmitted via satellite.

3. The method of claim 1, wherein the adapter card receives a series of frames representing a plurality of multiplexed data streams, thereby providing conditional access to each of the multiple data streams.

4. The method of claim 1, wherein each table entry of the Access Table further includes a key field for storing a Data Key corresponding to a data stream which the computer is authorized to receive, and the method further comprises the steps of:

    retrieving the table entry corresponding to the matching frame and table address; and

    if a match is found, decrypting the frame with the Data Key in the retrieved table entry.

5. The method of claim 4, further comprising the steps of:

    providing a User Key;

    receiving at least one Data Key, encrypted with the User Key;

    storing each Data Key in encrypted form in the Access Table; and

    decrypting the Data Key in the retrieved table entry with the User Key, before processing a frame for which a frame match is found.

6. The method of claim 4, wherein each table entry of the Access Table further includes a group field for storing a Group Key corresponding to a data stream which the computer is authorized to receive, and the method further comprises the steps of:

    providing a User Key;

    receiving at least one Group Key, encrypted with the User Key;

    receiving at least one Data Key, encrypted with the Group Key;

    storing each Group Key and Data Key in encrypted form in the Access Table; and

    decrypting the Group Key in the retrieved table entry with the User Key, and decrypting the Data Key in the retrieved table entry with the decrypted Group Key, before processing a frame for which a frame match is found.

7. The method of claim 1, further comprising the step of storing the processed frame in an output buffer prior to transmission to the computer.

8. The method of claim 1, further comprising the step of controlling, by the computer, the transmission of the processed frame to the computer.

9. The method of claim 1, further comprising the step of controlling, by the adapter card, the transmission of the processed frame to the computer.

10. A method for an adapter card for use in a computer, to process input data streams, wherein a data stream is comprised of at least one frame, for conditional access by the computer, and to process input data transmitted from the computer, comprising the steps of:

maintaining an Access Table, wherein each table entry includes an address field for storing an address corresponding to a data stream which the computer is authorized to receive;

receiving input data;

determining whether the input data contains data stream frames or computer data, wherein

if the input data contains data stream frames, for each frame:

determining an address of the frame;

determining whether the frame address matches an address maintained in the Access Table;

discarding the frame if a match is not found; and

processing the frame into output data if a match is found;

if the input data contains computer data, processing the computer data into output data; and

transmitting the output data to the computer via a bus interface.

11. The method of claim 10, wherein the data streams are transmitted via satellite.

12. The method of claim 10, wherein input data stream frames comprise a series of frames representing a plurality of multiplexed data streams, thereby providing conditional access to each of the multiple data streams.

13. The method of claim 10, wherein input data transmitted from the computer includes a data field, a key field, and an instruction field, and if the input data contains computer data, the step of processing the computer data into output data further comprises the steps of:

determining the operation to be performed based on the instruction field;

determining the key based on the key field;

determining the data based on the data field; and

performing the determined operation on the data with the key.

14. The method of claim 10, wherein each table entry of the Access Table further includes a key field for storing a Data Key corresponding to a data stream which the computer is authorized to receive, and the steps for processing data stream frames further comprise the steps of:

retrieving the table entry corresponding to the matching frame and table address; and

if a match is found, processing the frame by decrypting the frame with the Data Key in the retrieved table entry.

15. The method of claim 14, wherein the steps for processing data stream frames further comprise the steps of:

providing a User Key;

receiving at least one Data Key, encrypted with the User Key; and

decrypting the Data Key in the retrieved table entry with the User Key before processing a frame for which a frame match is found.

16. The method of claim 14, wherein each table entry of the Access Table further includes a group field for storing a Group Key corresponding to a data stream which the computer is authorized to receive, and the steps for processing data stream frames further comprise the steps of:

providing a User Key;

receiving at least one Group Key, encrypted with the User Key;

receiving at least one Data Key, encrypted with the Group Key;

storing each Group Key and Data Key in encrypted form in the Access Table; and

decrypting the Group Key in the retrieved table entry with the User Key, and decrypting the Data Key in the retrieved table entry with the decrypted Group Key, before processing a frame for which a frame match is found.

17. The method of claim 10, further comprising the step of providing an output buffer on the adapter card for storing the output data prior to transmission to the computer.

18. The method of claim 10, further comprising the step of controlling, by the computer, the transmission of the output data to the computer.

19. The method of claim 10, further comprising the step of controlling, by the adapter card, the transmission of the output data to the computer.

20. An adapter card for use in a computer, for providing conditional access by the computer to input data including data streams, wherein each data stream is comprised of at least one frame and each frame includes an address identifying the data stream, comprising:

a receiver for receiving a data stream frame;

an Access Table, wherein each table entry includes an address field for storing an address corresponding to a data stream which the computer is authorized to receive;

an integrated filter/crypto (IFC) block for determining an address of the received frame and determining whether the frame address matches an address maintained in the Access Table, wherein if a match is not found, the IFC block discards the frame, and if a match is found, the IFC block processes the frame into output data; and

a bus interface for transmitting the output data to the computer.

21. The adapter card of claim 20, wherein the input data comprises data streams transmitted via satellite.

22. The adapter card of claim 20, wherein the input data further includes data from the computer transmitted from the computer through the bus interface to the IFC block, and the IFC block processes the computer data into output data.

23. The adapter card of claim 22, wherein the input data from the computer includes data, information indicating a key, and an instruction indicating an operation to be performed on the data with the key, and the IFC block processes the computer data by performing the indicated operation with the indicated key on the data.

7

24. The adapter card of claim 20, wherein the IFC block is embodied in an ASIC.

25. The adapter card of claim 20, wherein:

each table entry of the Access Table further includes a key field for storing a Data Key corresponding to a data stream which the computer is authorized to receive; and

the IFC block retrieves the table entry corresponding to the frame address from the Access Table, and, if a match is found, uses the Data Key of the retrieved table entry to process the frame into output data.

26. The adapter card of claim 25, further comprising a User Key, stored on the adapter card, wherein the adapter card receives Data Keys encrypted with the User Key and stores each Data Key in the Access Table in encrypted form, and the IFC block decrypts the retrieved Data Key with the User Key and, if a match is found, uses the decrypted Data Key for processing the frame.

27. The adapter card of claim 25, further comprising a User Key, stored on the adapter card, wherein:

each table entry of the Access Table further includes a group field for storing a Group Key corresponding to a data stream which the computer is authorized to receive;

the adapter card receives at least one Group Key encrypted with the User Key and receives at least one Data Key encrypted with the Group Key, wherein each Group Key and each Data Key is stored in the Access Table in encrypted form; and

the IFC block decrypts the Group Key in the retrieved table entry with the User Key and decrypts the Data Key in the retrieved table entry with the decrypted Group Key, before processing a frame for which a frame match is found.

28. The adapter card of claim 20, further comprising an output buffer for storing the output data prior to transmission to the computer.

29. The adapter card of claim 20, wherein the computer controls the transmission of the output data to the computer via the bus interface.

30. The adapter card of claim 20, wherein the computer controls the transmission of the output data to the computer via the bus interface.

*   *   *   *   *