(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 698 21 183 T2** 2004.09.02

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 910 217 B1**
(21) Deutsches Aktenzeichen: **698 21 183.9**
(96) Europäisches Aktenzeichen: **98 402 444.8**
(96) Europäischer Anmeldetag: **05.10.1998**
(97) Erstveröffentlichung durch das EPA: **21.04.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **21.01.2004**
(47) Veröffentlichungstag im Patentblatt: **02.09.2004**

(51) Int Cl.[7]: **H04N 7/16**
H04N 7/167

(30) Unionspriorität:
9712837 **14.10.1997** **FR**

(84) Benannte Vertragsstaaten:
DE, FR, GB, IT

(73) Patentinhaber:
Thomson multimedia, Boulogne Billancourt, FR

(74) Vertreter:
Wördemann, H., Dipl.-Ing., Pat.-Anw., 31787 Hameln

(72) Erfinder:
Campinos, Arnaldo, 92100 Boulogne Billancourt, FR; Guillet, Dominique, 92100 Boulogne Billancourt, FR

(54) Bezeichnung: **Zugangskontrollverfahren für Hausnetz und Anordnung zu dessen Durchführung**

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein System für einen bedingten Zugriff und insbe sondere ein System für einen bedingten Zugriff für ein Heimnetz.

[0002] Ein System für einen bedingten Zugriff ermöglicht es einem Serviceanbieter, seinen Service nur zu den Benutzern zu liefern, die erworbene Berechtigungen zu diesem Service besitzen. Das ist z. B. der Fall in Gebührenfernsehsystemen. Ein Beispiel eines Systems für einen bedingten Zugriff ist beschrieben in dem Dokument US-A-5 420 866.

[0003] Wie dem Fachmann auf diesem Gebiet bekannt ist, besteht der durch einen Serviceanbieter gelieferte Service aus Informationen, die durch Steuerwörter verwürfelt sind. Das verwürfelte Datenwort kann entwürfelt und dadurch durch den Benutzer, nur zusammen mit den diesem Benutzer zugeordneten Berechtigungen, gelesen werden.

[0004] Zur Entwürfelung des Datenworts liefert der Serviceanbieter zu jedem Benutzer das Steuerwort, das für die Verwürfelung des Datenworts benutzt wird. Um die Steuerwörter geheim zu halten, werden sie geliefert, nachdem sie mit einem Algorithmus mit dem Schlüssel K verschlüsselt worden sind. Die verschiedenen verschlüsselten Steuerwörter werden zu den verschiedenen Benutzern in Steuernachrichten gesendet, die im Folgenden als ECM bezeichnet werden (ECM steht für "Entitlement Control Message").

[0005] Gemäß dem Stand der Technik besteht eine ECM aus einem Header und Nutzdaten.

[0006] Der Header gibt unter anderem den Typ und die Größe des Datenworts an, das in den Nutzdaten der ECM enthalten ist. Die Nutzdaten bestehen, unter anderem, aus einem Datenwort mit dem Satz von Bedingungen für den Zugriff zu dem durch den Anbieter gelieferten Service, einem Datenwort mit wenigstens einem Steuerwort, das mit dem Algorithmus mit dem Schlüssel K verschlüsselt ist, und einem Datenwort mit Daten, die von dem Schlüssel K abhängig sind und es ermöglichen, den Inhalt der ECM für gültig zu erklären oder zu validieren und zu prüfen, insbesondere die in dem ECM enthaltenen Zugriffsbedingungen.

[0007] Um den Zugriff zu seinem Service nur den berechtigten Benutzern zu gewähren, liefert der Serviceanbieter eine Smart Card und einen Decoder zu jedem der Benutzer.

[0008] Die Smart Card ermöglicht einerseits die Berechtigungen zu validieren oder für gültig zu erklären und aufzuzeichnen, die der Benutzer zu dem gelieferten Service hat, und andererseits mit Hilfe des Schlüssels K die verschlüsselten Steuerwörter zu entschlüsseln. Zu diesem Zweck enthält die Smart Card den Schlüssel K des Algorithmus, der die Verschlüsselung der Steuerwörter ermöglicht hat.

[0009] Der Decoder ermöglicht es für seinen Teil, das verwürfelte Datenwort auf der Grundlage des Datenworts aus den verschlüsselten Steuerwörtern von der Smart Card zu entwürfeln.

[0010] Diese Berechtigungen jedes Benutzers werden in Nachrichten für die Verwaltung der Berechtigungen des Benutzers gesendet, die daraufhin durch die EMM bezeichnet werden (die Abkürzung EMM steht für "Entitlement Management Message").

[0011] Gemäß dem Stand der Technik besteht eine Nachricht EMM aus einem Header und Nutzdaten. Die Nutzdaten der EMM enthalten drei Hauptpunkte.

- ein erstes Datenwort, das die Adresse der Benutzerkarte angibt,
- ein zweites Datenwort, das die Beschreibung der Berechtigungen des Benutzers angibt,
- ein drittes Datenwort, das es ermöglicht, die EMM für gültig zu erklären oder zu validieren und zu prüfen, ob die Berechtigungen des Benutzers der EMM tatsächlich die für den Benutzer reservierten Berechtigungen sind.

[0012] Wie vorangehend erwähnt, werden die verschlüsselten Steuerwörter durch die ECMs zu den Benutzern gesendet.

[0013] Wenn der Decoder eines Benutzers die Adresse der zugehörigen Karte und den verschiedenen, über den Serviceanbieter verteilten Adressen zugeordnet sind, wird die EMM entsprechend der erkannten Adresse analysiert. Die Analyse der EMM erfolgt mittels eines Analysealgorithmus, der durch den Verschlüsselungsschlüssel K der Steuerwörter gesteuert wird.

[0014] Wenn die Analyse der Nachricht EMM zu der Gültigkeitserklärung des Letzteren führt, dann werden die Berechtigungen des Benutzers in einem Speicher gespeichert.

[0015] Die Benutzerkarte enthält außerdem eine Schaltung zur Gültigkeitserklärung der ECMs, eine Schaltung für die Zugriffssteuerung und außerdem eine Schaltung zur Entschlüsselung der verschlüsselten Steuerörter.

[0016] Die Schaltung zur Validierung der ECMs ermöglicht, die Zugriffsbedingungen zu validieren. Die Zugriffssteuerungsschaltung vergleicht die validierten Zugriffsbedingungen mit den validierten Berechtigungen des Benutzers. Wenn die validierten Zugriffsbedingungen den validierten Berechtigungen des Benutzers entsprechen, dann wird die Entschlüsselung freigegeben oder autorisiert. Im entgegengesetzten Fall wird die Entschlüsselung nicht autorisiert.

[0017] Ein Heimnetz besteht aus einem Satz von Heim-Terminals, die miteinander über einen Heimbus verbunden sind, wie z. B. dem Bus IEEE 1394.

[0018] Der Ausdruck Heim-Terminal von anhand von nicht-einschränkenden Beispielen einen Empfänger von Fernsehprogrammen, einen digitalen Decoder, einen digitalen Camcorder, einen Leser für digitale Platten, allgemein mit DVDs bezeichnet (die Abkürzung DVD steht für "Digital Versatile Disc") oder ansonsten ein Terminal bedeuten, das allgemein bezeichnet wird als ein PC (die Abkürzung PC steht für "Personal Computer").

[0019] Im Rahmen eines Systems für einen beding-

ten Zugriff, wie ein solcher gemäß dem oben genannten Stand der Technik, wenn ein Serviceanbieter-Abonnent z. B. dasselbe Programm auf allen Fernsehempfängern empfangen möchte, dann wird er gezwungen, so viele Abonnenten aufzunehmen, wie er Fernsehempfänger hat. Aus der Sicht des Benutzers bildet dieses einen Hauptnachteil hinsichtlich der Kosten.

[0020] Aus der Sicht des Serviceanbieters stellt dieses ebenfalls einen Hauptnachteil dar. Das ist der Fall, weil es für den Serviceanbieter unmöglich ist, seine Dienstleistungen selektiv hinsichtlich des gesamten Speichervolumens der Programmempfänger und im Allgemeinen vom Heim-Terminal vorzunehmen, die der Abonnent besitzt.

[0021] Die Erfindung weist diese Nachteile nicht auf.

[0022] Die Erfindung betrifft ein Verfahren zur Zugriffssteuerung zu einem durch ein erstes Gerät verwürtelten Datenwort. Das Verfahren enthält folgende Schritte: (a) Empfang eines Datenstroms über ein Front-End in dem ersten Gerät mit: dem verwürfelten Datenelement, verwürfelt durch Anwendung eines Steuerworts das durch einen Schlüssel verschlüsselten ist, und (b) Entschlüsselung des verschlüsselten Steuerworts in dem ersten Gerät, um das Steuerwort zurückzugewinnen. Gemäß einem ersten Aspekt der Erfindung ist das erste Gerät mit einem lokalen Netz verbunden und enthält die folgenden Schritte: (c) Übertragung des verwürtelten Datenelements über das lokale Netz zu einem zweiten Gerät, (d) Erzeugung eines Entwürtelungs-Datenelements mit dem Steuerwort, dem Datenwort zur Identifizierung des verwürfelten Datenelements und der Adresse des zweiten Geräts und (e) Übertragung des Entwürtelungs-Datenelements über das lokale Netz zu dem zweiten Gerät.

[0023] Gemäß einem besonderen Aspekt der Erfindung erfolgt der Schritt (e) asynchron mit dem Schritt (c).

[0024] Gemäß einem anderen Aspekt der Erfindung enthält der Schritt (c): Übertragung des verwürtelten Datenelements zu dem zweiten Gerät durch den isochronen Kanal eines Bus, der das erste und zweite Gerät miteinander verbindet.

[0025] Gemäß einem weiteren Aspekt der Erfindung enthält der Schritt (e) Folgendes: Übertragung des Entwürfelungs-Datenelements zu dem zweiten Gerät durch Anwendung des asynchronen Kanals des Bus.

[0026] In einer besonderen Ausführungsform der Erfindung enthält der beim Schritt (a) empfangene Datenstrom außerdem die Berechtigungen des Benutzers für das verwürfelte Datenelement, wobei die Berechtigungen die Neuverteilungs-Berechtigungen für die Verteilung des verwürfelten Datenelements in dem lokalen Netz enthalten sind. In dieser Ausführungsform enthält das Verfahren außerdem den Schritt für: (f) Speicherung der Neuverteilungs-Berechtigungen in dem ersten Gerät, (g) Empfang eines Befehls mit der Adresse des zweiten Geräts von einem zweiten Gerät über das lokale Netz und (h) Vergleich des Befehls mit den gespeicherten Neuverteilungs-Berechtigungen, um die Übertragung des verwürfelten Datenelements zu dem zweiten Gerät um das Entwürfelungs-Datenelement bei den Schritten (c) und (e) zu autorisierten oder nicht zu autorisieren.

[0027] Gemäß einem besonderen Aspekt der Erfindung wird das in dem Entwürfelungs-Datenelement enthaltene Steuerwort bei dem lokalen Netz verschlüsselt.

[0028] Die Erfindung betrifft außerdem ein Verfahren zur Verwaltung des Zugriffs zu einem verwürfelten Datenelement in einem lokalen Netz mit folgenden Schritten: (i) Empfang in einem ersten Terminal über das lokale Netz eines durch Anwendung eines Steuerworts verwürfelten Datenelements und eines Entwürfelungs-Datenele-ments, das das Steuerwort ein Datenwort zur Identifizierung des verwürfelten Datenelements und der Adresse eines mit dem Netz verbundenen Terminals (j) Vergleich der in dem Entwürfelungs-Datenelement enthaltenen Adresse mit der Adresse des Terminals und, wenn die Adressen übereinstimmen, Autorisierung des ersten Terminals zur Entwürfelung des verwürfelten Datenelements unter Anwendung des in dem Entwürfelungs-Datenelement enthaltenen Steuerworts.

[0029] Die Erfindung betrifft außerdem ein Gerät zur Steuerung des Zugriffs zu einem verwürfelten Datenelement durch ein Terminal, wobei das Gerät Mittel zum Empfang eines Datenstroms über ein Front-End mit folgenden Merkmalen enthält: ein verwürfeltes Datenelement, das durch ein Steuerwort verwürfelt ist, das durch einen Schlüssel verschlüsselte Steuerwort und ein Datenwort zur Identifizierung des verwürfelten Datenelements, wobei das Gerät Mittel zur Entschlüsselung des verschlüsselten Datenworts zur Wiedergewinnung des Steuerworts enthält. Gemäß diesem Aspekt der Erfindung enthält das Gerät außerdem: Mittel zur Bildung eines Entwürfelungs-Datenelements, das das Steuerwort, das Datenwort zur Identifizierung des verwürfelten Datenelements und die Adresse des Terminals und Mittel zur Übertragung des verwürfelten Datenelements und des Entwürfelungs-Datenelements über ein lokales Netz zu dem Terminal enthält.

[0030] Gemäß einer besonderen Ausführungsform der Erfindung enthalten die Übertragungsmittel einen Datenbus, der eine asynchrone Verbindung enthält, über die das Entschlüsselungs-Datenelement weitergeleitet wird.

[0031] Die Erfindung wird genauer beschrieben, in dem Fall, in dem der bedingte Zugriff ein Netz von Heim-Terminals betrifft, die über einen Bus miteinander verbunden sind. Allgemeiner betrifft die Erfindung jedoch den Fall, in dem der bedingte Zugriff wenigstens ein Benutzerterminal betrifft, das als Netz oder auf andere Weise ausgebildet ist.

[0032] Die Erfindung ermöglicht es in vorteilhafter Weise einem Serviceanbieter, seinen Service selektiv für einen Satz von vernetzten Heimterminals zu

wählen.

[0033] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus einer bevorzugten Ausführungsform der Erfindung anhand der beigefügten Figuren:

[0034] **Fig.** 1 zeigt ein Gerät für ein System mit einem bedingten Zugriff mit Mitteln, die es ermöglichen, den Zugriff durch wenigstens ein Programm bei dem wenigstens einen Heimterminal zu steuern, gemäß der Erfindung,

[0035] **Fig.** 2 zeigt gemäß der Erfindung ein Entwürfelungs-Datenelement, das es ermöglicht, ein verwürfeltes Datenelement zu entwürfeln,

[0036] **Fig.** 3 zeigt ein Gerät zur Entwürfelung wenigstens eines verwürfelten Programms, das mittels eines Gerätes für ein System mit einem bedingten Zugriff ausgewählt wurde, wie dasjenige, das in **Fig.** 1 dargestellt ist.

[0037] In allen Figuren bezeichnen gleiche Bezugszeichen gleiche Elemente.

[0038] **Fig.** 1 zeigt ein Gerät für ein System mit einem bedingten Zugriff mit Mitteln, die es ermöglichen, den Zugriff durch wenigstens ein Programm auf wenigstens einem Heimterminal zu steuern, gemäß der Erfindung.

[0039] Das Gerät D1 für ein System mit einem bedingten Zugriff enthält eine Demultiplexschaltung **1**, eine Schaltung **3** zur Schnittstellenbildung mit einem Heimbus B, einen Mikroprozessor **2** und eine Schaltung **4** für die Schnittstellenbildung zwischen dem Mikroprozessor **2** und der Smart Card **5**.

[0040] Die Demultiplexschaltung **1** empfängt an ihrem Eingang den Datenstrom F entsprechend allen Programmen, die durch den Serviceanbieter verteilt werden. Vorzugsweise geht der Strom F von einer Analog/Digital-Umsetzschaltung aus (in **Fig.** 1 nicht dargestellt), die allgemein als ein "Front-End" bezeichnet wird.

[0041] Wie es dem Fachmann auf diesem Gebiet bekannt ist, enthält in dem Fall eines Datentransports im MPEG-Format der Strom F eine Aufeinanderfolge von Paketen aus Videodaten, Paketen aus Audiodaten und Paketen von Verwaltungsdaten, wie z. B. die Daten in den ECMs und den EMMs.

[0042] Jedes Datenpaket enthält in seinem Header einen Identifizierer, der im Folgenden mit PID bezeichnet wird (die Abkürzung PID steht für "Packet Identifier"), der es ermöglicht, sowohl die Art der in dem Paket enthaltenen Daten (Video, Audio oder Verwaltung) und das Programm zu identifizieren, zu dem dieses Paket gehört.

[0043] Jedes durch den Serviceanbieter gelieferte Programm besteht aus einem Satz von Programmkomponenten, und jede Programmkomponente besteht aus einem Satz von Paketen, deren PIDs identisch sind.

[0044] Der Strom F enthält außerdem ein Datenelement, das im Folgenden als eine PMT-Tabelle bezeichnet wird (die Abkürzung PMT steht für "Programme Map Table") und das die PIDs sammelt, die dem Satz von Programmen entsprechen, die durch den Serviceanbieter verteilt werden.

[0045] Gemäß der Erfindung erzeugt der Mikroprozessor **2** durch die Wirkung eines Befehls CD1 einen Befehl CD2, der dem Demultiplexer **1** zugeführt wird. Der Befehl CD1 ist ein Benutzerbefehl, der in einer für sich bekannten Weise von der Interaktion eines Benutzers mit einem Heimterminal ausgeht. Der Befehl CD1 kann auf verschiedene Weise zu dem Mikroprozessor **2** übertragen werden. Gemäß einer ersten Ausführungsform kann der Befehl CD1 von dem Heimterminal für den Mikroprozessor **2** über einen Heimbus B übertragen werden. Gemäß einer anderen Ausführungsform kann der Befehl CD1 einer Steuerschnittstelle zugeführt werden, die in **Fig.** 1 nicht dargestellt ist und die ein Teil des Gerätes D1 sein kann oder auch nicht. Der Befehl CD1 enthält ein Adressendatenwort AD für das Heimterminal, auf dem der Benutzer das Programm empfangen möchte, das er auswählt. Beim Empfang des Befehls CD1 wird das Adressendatenwort AD in dem Mikroprozessor **2** gespeichert.

[0046] Die dem gewählten Programm entsprechende PMT-Tabelle wird in für sich bekannter Weise aus dem Strom F extrahiert und zu dem Mikroprozessor **2** weitergeleitet. Der Mikroprozessor **2** verarbeitet das durch die PMT-Tabelle dargestellte Datenelement und extrahiert daraus die PIDs des gewählten Programms. Die extrahierten PIDs werden dann von dem Mikroprozessor **2** zu dem Demultiplexer **1** weitergeleitet. Unter der Wirkung der PIDs wählt der Demultiplexer **1** den Strom der verwürfelten Daten FS, die dem gewählten Programm entsprechen, die verschiedenen Nachrichten ECM, die die Steuerwörter enthalten, die es ermöglichen, das gewählte Programm zu entwürfeln, sowie die Nachrichten EMM, die die Berechtigungen des Benutzers für die durch den Anbieter gelieferten Servicedienste enthalten.

[0047] Der Strom FS wird von dem Demultiplexer **1** zu der Schnittstellenschaltung **3** weitergeleitet, und die Nachrichten ECM und EMM werden von dem Demultiplexer **1** über den Mikroprozessor **2** und die Schnittstellenschaltung **4** zu der Smart Card **5** weitergeleitet.

[0048] Wie es dem Fachmann auf diesem Gebiet bekannt ist, enthält die Smart Card **5** fünf Hauptschaltungen (in **Fig.** 1 nicht dargestellt):

- eine Schaltung zur Validierung der Berechtigungen des Benutzers,
- eine Schaltung zum Speichern der validierten Berechtigungen des Benutzers,
- eine Zugriffssteuerschaltung,
- eine Schaltung zur Validierung der Nachrichten ECM,
- eine Schaltung zur Entschlüsselung der verschlüsselten Steuerwörter.

[0049] Wie bereits erwähnt, ermöglicht die Validierungsschaltung, für die Nachrichten EMM die Vorgänge für die Erkennung der Adresse des Benutzers und zur Analyse der Berechtigungen des Benutzers

zu erkennen. Zu diesem Zweck enthält die Validierungsschaltung den Schlüssel K des Algorithmus für die Verschlüsselung der Steuerwörter. Wenn die Nachricht EMM validiert ist, werden die in der Nachricht EMM enthaltenen Benutzerberechtigungen in der Schaltung zur Speicherung der validierten Berechtigungen gespeichert.

[0050] Gemäß der Erfindung werden in dem Fall, in dem die Heimterminals vernetzt sind, die validierten Berechtigungen des Benutzers aufgeteilt, vorzugsweise in zwei Kategorien:

– eine erste Kategorie von Berechtigungen betrifft die eigenen Berechtigungen, die ein Benutzer besitzt, bezüglich wenigstens eines durch den Serviceanbieter verteilten Programms,

– eine zweite Kategorie von Berechtigungen betrifft die Neuverteilungs-Berechtigungen, die der Serviceanbieter einem Benutzer in dem Heimnetz des Benutzers gewährt.

[0051] Gemäß einem nicht-einschränkenden Beispiel kann die Neuverteilungs-Berechtigung, die ein Serviceanbieter einem Benutzer in diesem Heimnetz gewährt, die Form einer Anzahl von unterschiedlichen Terminals annehmen, auf denen der Serviceanbieter den Benutzer autorisiert, ein Programm zu empfangen. Es kann ebenso eine Maximalzahl von verschiedenen Programmen sein, für die der Serviceanbieter einen unverschlüsselten Empfang autorisiert, unabhängig davon, um welche Programme es sich handelt.

[0052] Wie bereits erwähnt, macht die Schaltung zur Validierung der ECMs es möglich, die Zugriffsbedingungen zu validieren, die in den ECMs enthalten sind. Zu diesem Zweck enthält die Schaltung zur Validierung der ECMs den Schlüssel K des Algorithmus für die Verschlüsselung der Steuerwörter.

[0053] Somit vergleicht die Zugriffssteuerschaltung die Bedingungen für den validierten Zugriff mit den validierten Berechtigungen des Benutzers mit der ersten Kategorie der oben genannten Berechtigungen.

[0054] Wenn die validierten Zugriffsbedingungen den validierten Berechtigungen des Benutzers entsprechen, wird die Entschlüsselung der Steuerwörter autorisiert. In dem entgegengesetzten Fall wird die Entschlüsselung nicht autorisiert.

[0055] In dem Fall, in dem die Entschlüsselung der verschlüsselten Steuerwörter autorisiert ist, werden die entschlüsselten Steuerwörter CW über die Schnittstellenschaltung **4** von der Smart Card **5** zu dem Mikroprozessor **2** weitergeleitet.

[0056] Jedes entschlüsselte Steuerwort CW macht es möglich, das durch eine Programmkomponente gebildete verwürfelte Element zu entwürfeln. Wie erwähnt, besteht jede Programmkomponente aus einem Satz von Paketen, deren PIDs identisch sind. Daraus folgt, dass jedem Steuerwort CW ein PID entspricht, der im Folgenden mit PID (CW) bezeichnet wird und es ermöglicht, das verwürfelte Element zu identifizieren.

[0057] Gemäß der Erfindung bildet der Mikroprozessor **2** für jedes entschlüsselte Steuerwort ein Entwürfelungselement I mit dem entschlüsselten Steuerwort CW, das Datenwort PID (CW), das es ermöglicht, die zu entwürfelnde Identität der Programmkomponente und das Adressendatenwort AD des Heimterminals, von dem der Befehl für den Zugriff zu dem gewählten Programm ausgeht, zu identifizieren.

[0058] Wie dem Fachmann auf diesem Gebiet bekannt ist, gibt es Fälle, für die eine einzelne Nachricht ECM zwei Steuerwörter enthält. Ein erstes Steuerwort ist ein solches, das es ermöglicht, die Komponente des Programms zu entwürfeln, das derzeit gelesen wird, und ein zweites Steuerwort, das es ermöglicht, die Komponente des Programms zu entwürfeln, die auf die Komponente des derzeit gelesenen Programms folgt. Gemäß der Erfindung enthält vorzugsweise in Fällen wie dem oben genannten das Element I ein zusätzliches Datenwort, das es ermöglicht, anzuzeigen, ob das entschlüsselte Steuerwort, das es enthält, von dem ersten Typ oder von dem zweiten Typ ist.

[0059] In einer für sich bekannten Weise enthält das Datenelement I außerdem einen Header H, der es unter anderem ermöglicht, den Typ und die Größe des Datenwortes, das es enthält, zu definieren.

[0060] Die Schnittstellenschaltung **3** empfängt den durch den Demultiplexer ausgegebenen Strom FS ebenso das durch den Mikroprozessor **2** ausgegebene Element I.

[0061] Gemäß einer ersten Ausführungsform der Erfindung werden die Neuverteilungs-Berechtigungen DR für die Programme, die in der Smart Card **5** gespeichert sind, über die Schnittstelle **4** und den Mikroprozessor **2** zu einer Speicherschaltung übertragen, die z. B. in der Schnittstellenschaltung **3** liegt. Die Kopierung der Berechtigungen DR in eine Speicherschaltung kann einmal und für alle erfolgen, sie kann aber in vorteilhafter Weise immer dann erfolgen, wenn diese Berechtigungen geändert werden.

[0062] Wenn die Neuverteilungs-Berechtigungen DR für die durch den Serviceanbieter gelieferten Programme so autorisieren, die Anforderung für ein Programm, dessen Entwürfelung sich selbst autorisiert, nimmt eine Form der Weiterleitung zu dem Heimterminal an, von dem die Anforderungen ausgehen, über den Heimbus B des gewählten Stroms FS und der verschiedenen Datenelemente I, die die Adresse des Heimterminals enthalten. Die Autorisierung zur Verteilung der Programme in dem Heimnetz wird durch ein Signal gesteuert, das aus dem Vergleich zwischen den Berechtigungen DR und den verschiedenen Befehlen stammt, über den Bus B von den Heimterminals. Die Komparatorschaltung, die diesen Vergleich durchführt, kann z. B. in der Schnittstellenschaltung **3** enthalten sein.

[0063] Gemäß einer zweiten Ausführungsform der Erfindung werden die Berechtigungen DR nicht zu einer Speicherschaltung übertragen, wie oben erläu-

tert. Es sind die verschiedenen Befehle TD von den Heimterminals, die übenden Mikroprozessor **2** und die Schnittstelle **4** zu einem Speicherbereich der Smart Card **5** übertragen werden. Der Vergleich der Berechtigungen DR und der Befehle TD von den Heimterminals erfolgt dann soweit durch eine Vergleichsschaltung, so wie z. B. die Zugriffssteuerschaltung in der Smart Card **5**. Ein Signal S aus dem Vergleich zwischen den Berechtigungen DR und den Befehlen TD werden über die Schnittstellenschaltung **4** von der Smart Card **5** zu dem Mikroprozessor **2** übertragen, der dann einen Befehl CS erzeugt, der es ermöglicht, ganz oder teilweise die Programmanforderungen von den Heimterminals zu autorisieren oder nicht.

[0064] Gemäß der Erfindung bildet das Datenelement I, das die Entwürfelung eines Programms ermöglicht, keinen Teil des Stroms FS in dem MPEG2-Format. Das Datenelement I läuft über die asynchrone Strecke des Heimbus B und wird nur zu dem Terminal weitergeleitet, von dem die Programmanforderungen ausgehen. Dieser Strom FS läuft vorzugsweise über die isochrone Strecke des Bus B. In vorteilhafter Weise ist es dann gemäß der Erfindung nicht notwendig, dass die Steuerwörter, die um das Heimnetz laufen, verschlüsselt werden.

[0065] Gemäß der Erfindung werden die entschlüsselten Steuerwörter, die um das Heimnetz herumlaufen, nicht mehr mit den Daten synchronisiert, die sie in derselben Weise wie im Stand der Technik entschlüsselt müssen. In vorteilhafter Weise ist es jedoch nicht notwendig, spezielle Signale vorzusehen, um die Synchronisierung eines Steuerworts und der Programmkomponente zu erreichen, zu dem dieses Steuerwort entwürfelt werden muss. Wenn die Bitraten durch den asynchronen Kanal des Bus erlaubt sind (in dem Beispiel des Bus IEEE 1394, diese Bitrate beträgt ungefähr 4 Mbyte/s), wird diese Synchronisierung ohne Schwierigkeit bewirkt.

[0066] Gemäß der Erfindung kann ein Gerät für ein System für einen bedingten Zugriff, wie dasjenige in **Fig.** 1, in demselben Decoder verschiedenen Schaltungen zugeordnet werden, die die lokale Entwürfelung der verwürfelten Daten ermöglichen. Der Ausdruck lokale Entwürfelung der verwürfelten Daten soll so verstanden werden, dass er eine Entwürfelung von Daten in dem Decoder selbst bedeutet. Ein derartiger Decoder kann in bekannter Weise eine Entwürtelungs-schaltung, eine Demultiplexerschaltung und einen Video- und Audiodecoder im MPEG2-Format enthalten. Die lokal entwürfelten Daten werden vorzugsweise in derselben Weise entwürfelt, wie sie vorangehend gemäß dem Stand der Technik beschrieben wurden.

[0067] Wie oben erwähnt, kann vorzugsweise ein Decoder, wie er oben beschrieben wurde, außerdem an seinem Eingang einen Analog/Digital-Konverter enthalten, der allgemein als "Front-End" bezeichnet wird.

[0068] **Fig.** 2 zeigt, gemäß der Erfindung, ein Entwürfelungs-Datenelement, das es ermöglicht, ein verwürfeltes Datenelement zu entwürfeln.

[0069] Das in **Fig.** 2 dargestellte Datenelement ist das obengenannte Datenelement I.

[0070] Das Datenelement I bildet eine Nachricht mit einem Header **6**, dessen Inhalt H es unter anderem ermöglicht, den Typ und die Größe der in der Nachricht enthaltenen Daten zu bestimmen, ein Datenwort **7** mit der Adresse AD eines Heimterminals, das eine Anforderung für den Zugriff zu einem Programm gesendet hat, ein Datenwort **8** mit einem entschlüsselten Steuerwort CW, vorgesehen zum Entwürfeln einer Programmkomponente, ein Datenwort **9** mit dem Datenwort PID (CW) und, gemäß einer besonderen Ausführungsform der Erfindung, ein Datenwort **10** mit einem Datenelement X, das es ermöglicht, anzuzeigen, ob das Steuerwort CW ein Steuerwort des ersten Typs oder des zweiten Typs ist. Gemäß anderen Ausführungsformen der Erfindung enthält das Datenelement I nicht das Datenwort **10**.

[0071] **Fig.** 3 zeigt ein Gerät für die Entwürfelung wenigstens eines verwürtelten Programms, das mittels eines Gerätes für ein System mit bedingtem Zugriff gewählt wurde, wie dasjenige, das in **Fig.** 1 dargestellt ist. Gemäß der Erfindung gehört ein derartiges, in der **Fig.** 3 dargestelltes Gerät zu einem Heimterminal.

[0072] Das Entwürfelungsgerät D2 enthält eine Schnittstellenschaltung **11**, eine Entwürfelungs- und Demultiplexing-Schaltung **12** und einen Video- und Audiodecoder **13**.

[0073] Die Schnittstellenschaltung **11** ist über wenigstens zwei Zugriffsanschlüsse mit dem Heimbus B verbunden. Durch einen ersten Zugriffsanschluss A1 empfängt die Schnittstellenschaltung **11**, in für sich bekannter Weise, den Datenstrom, der durch das Heimterminal gewählt wurde, zu dem er gehört, sowie auch den Datenstrom oder die Datenströme, die durch das Heimterminal oder die Terminals vor dem Heimterminal ausgewählt wurden, zu dem er gehört. Gemäß der Erfindung empfängt die Schaltung **11** außerdem über den ersten Zugriffsanschluss A1 die verschiedenen Entwürfelungs-Datenelemente I, die dem Satz der gewählten Programme entsprechen.

[0074] In dem Fall, wenn die Schnittstellenschaltung **11** aus den Entwürfelungs-Datenelementen I erkennt, welche er empfängt, wählen die Datenelemente IT mit der Adresse des Heimterminals, zu dem es gehört, diese aus und leiten sie zu der Schaltung **12** weiter. Die Datenelemente IT enthalten die Gesamtheit der Datenelemente, die für die Parametrisierung, die Entwürfelungsschaltung **12** (CW, PID (CW)), X).

[0075] Der Datenstrom FST, der dem erkannten Datenelement IT entspricht, wird zu der Entwürfelungs- und Demultiplexing-Schaltung **12** weitergeleitet. Unter der Wirkung der Steuerwörter CW werden die verwürfelten Daten des Stroms FST entwürfelt. In einer für sich bekannten Weise werden die entwürfelten Daten so demultiplexiert, dass die Video- und Audiodaten in dem MPEG2-Format rekonstruiert werden.

Die Video- und Audiodaten in dem MPEG2-Format werden dann von der Schaltung **12** zu dem Video- und Audiodecoder **13** weitergeleitet. Die von dem Video- und Audiodecoder **13** ausgegebenen Daten werden dann zu dem Heimterminal weitergeleitet, zu dem das Gerät D2 gehört.

[0076] In dem Fall, wenn die Schnittstellenschaltung **11** einen verwürfelten Datenstrom empfängt, der durch ein Heimterminal ausgewählt wird, das im Signalweg vor dem Heimterminal liegt, zu dem es gehört, wird dieser Datenstrom sowie die Nachrichten vom Typ I mit den Steuerwörtern für die Entwürfelung zu dem zweiten Zugriffsanschluss A2 gelenkt und über das Heimnetz weitergeleitet.

[0077] Durch den mit dem Zugriffsanschluss A2 verbundenen Heimbus B werden der Strom von verwürfelten Daten sowie die Nachrichten vom Typ I mit den Steuerwörtern für die Entwürfelung des Datenstroms zu dem Entwürfelungsgerät weitergeleitet, zu dem das Heimterminal gehört, von dem die Programmanforderung ausgeht.

[0078] Gemäß der Erfindung erfolgt die Zugriffssteuerung in ihrer Gesamtheit durch das Gerät D1. Jedes Entschlüsselungsgerät für ein Heimterminal ist somit unabhängig von dem Zugriffssteuersystem, mit dem es verbunden ist. In vorteilhafter Weise folgt daraus, dass das Heimnetz kompatibel ist mit zahlreichen anderen Systemen für einen bedingten Zugriff.

[0079] Wie früher erwähnt, sind die Steuerwörter, die um das Heimnetz laufen, Steuerwörter, die von einem Betrieb für die Entschlüsselung der verschlüsselten Steuerwörter ausgehen, die durch einen Serviceanbieter geliefert werden. Somit sind gemäß der bevorzugten Ausführungsform der Erfindung die Steuerwörter, die um das Heimnetz herumlaufen, nicht-verschlüsselte Steuerwörter.

[0080] Die Erfindung betrifft jedoch auch den Fall, in dem die Steuerwörter, die um das Heimnetz laufen, verschlüsselte Steuerwörter sind. Die Verschlüsselung der Steuerwörter ist dann eine Verschlüsselung, die beim Heimnetz selbst durch ein Verschlüsselungsgerät erfolgt, das vorzugsweise bei dem Kopf oder Head des Netzes liegt. Die Verschlüsselung der Steuerwörter, die um das Heimnetz laufen, findet einen besonderen Vorteil in Fällen, in denen der Benutzer des Heimnetzes wünscht, den Wert des Schutzes der Datenelemente erhöhen, die um das Netz herumlaufen. In dem Fall, in dem die Steuerwörter, die um das Heimnetz herumlaufen, verschlüsselt sind, enthält jedes Entwürtelungsgerät eine Schaltung, die es ermöglicht, sie zu entschlüsseln, bevor der Entwürfelungsvorgang erfolgt.

Patentansprüche

1. Verfahren zur Steuerung des Zugriffs zu einem über ein erstes Gerät (D1) empfangenes verwürfeltes Datenelement (FS) mit folgenden Schritten:

(a) Empfang eines Datenstroms (F) über ein Front-End in dem ersten Gerät (D1) mit:

– dem durch Anwendung eines Steuerworts (CW) verwürfelten Verwürfelungs-Datenelement (FS),

– dem durch Anwendung eines Schlüssels (K) verschlüsselten Steuerwort, und

– einem Datenwort (PID(CW)), das es ermöglicht, das verwürfelte Datenelement zu identifizieren,

(b) Entschlüsselung des verschlüsselten Steuerworts in dem ersten Gerät (D1), um das Steuerwort (CW) zurückzugewinnen,

gekennzeichnet durch

die Tatsache, dass das erste Gerät mit einem lokalen Netz verbunden ist, und durch folgende Schritte:

(c) Übertragung des verwürfelten Datenelements (FS) über das lokale Netz zu einem zweiten Gerät (D2),

(d) Erzeugung eines Entwürfelungs-Datenelements (I) mit dem Steuenrwort (CW), dem Datenwort (PID(CW)) zur Identifizierung des verwürfelten Datenelements und der Adresse (AD) des zweiten Geräts und

(e) Übertragung des Entwürfelungs-Datenelements (I) über das lokale Netz zu dem zweiten Gerät (D2).

2. Verfahren nach Anspruch 1, wobei der Schritt (e) asynchron mit dem Schritt (c) durchgeführt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, wobei der Schritt (c) folgendes enthält:

Übertragung des verwürfelten Datenelements (FS) zu dem zweiten Gerät (D2) durch Anwendung des isochronen Kanals eines Bus (B), der das erste und das zweite Gerät miteinander verbindet.

4. Verfahren nach Anspruch 3, wobei der Schritt (e) folgendes enthält:

Übertragung des Entwürfelungs-Datenelements (I) zu dem zweiten Gerät (D2) durch Anwendung des asynchronen Kanals des Bus (B).

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der beim Schritt (a) empfangene Datenstrom (F) außerdem die Berechtigungen des Benutzers für das verwürfelte Datenelement (FS) enthält, dass die Berechtigungen die Neuverteilungs-Berechtigungen (DR) für die Verteilung des verwürfelten Datenelements in dem lokalen Netz enthalten, und

wobei das Verfahren außerdem folgende Schritte enthält:

(f) Speicherung der Neuverteilungs-Berechtigungen (DR) in dem ersten Gerät (D1),

(g) Empfang eines Befehls (TD) mit der Adresse (AD) des zweiten Geräts von einem zweiten Gerät (D2) über das lokale Netz und

(h) Vergleich des Befehls (TD) mit den gespeicherten Neuverteilungs-Berechtigungen (DR), um die Übertragung des verwürfelten Datenelements (FS) zu dem zweiten Gerät und das Entwürfelungs-Datenelement (I) bei den Schritten (c) und (e) zu autorisieren oder nicht zu autorisieren.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass das in dem Entwürfelungs-Datenelement (I) enthaltene Steuerwort bei dem lokalen Netz verschlüsselt wird.

7. Verfahren zur Verwaltung des Zugriffs zu einem verwürfelten Datenelement in einem lokalen Netz mit folgenden Schritten:
(a) Empfang in einem mit dem lokalen Netz verbundenen ersten Terminal:
– eines durch Anwendung eines Steuerworts (CW) Verwürfelungs-Datenelements (FS), und
– eines Entwürfelungs-Datenelements (I), das das Steuerwort (CW), ein Datenwort (PID(CW)) zur Identifizierung des verwürfelten Datenelements und die Adresse (AD) eines mit dem Netz verbundenen Terminals enthält,
(b) Vergleich der in dem Entwürfelungs-Datenelement (I) enthaltenen Adresse mit der Adresse des ersten Terminals und,
wenn die Adressen übereinstimmen, Autorisierung des ersten Terminals zur Entwürfelung des verwürtelten Datenelements unter Anwendung des in dem Entwürtelungs-Datenelement enthaltenen Steuerworts.

8. Gerät (D1) zur Steuerung des Zugriffs zu einem verwürfelten Datenelement durch ein Terminal (D2), wobei das Gerät Mittel zum Empfang eines Datenstroms (F) von einem Front-End enthält, mit folgenden Merkmalen:
– ein verwürfeltes Datenelement (FS), das durch ein Steuerwort (CW) verwürfelt ist,
– das durch einen Schlüssel (K) verschlüsselte Steuerwort und
– ein Datenwort (PID(CW)) zur Identifizierung des verwürfelten Datenelements,
wobei das Gerät Mittel (**5**) zur Entschlüsselung des verschlüsselten Steuerworts zur Wiedergewinnung des Steuerworts enthält, gekennzeichnet durch:
Mittel (**2**) zur Bildung eines Entwürfelungs-Datenelements (I), das das Steuerwort (CW), das Datenwort (PID(CW)) zur Identifizierung des verwürtelten Datenelements und die Adresse (AD) des Terminals enthält, und
Mittel zur Übertragung des verwürfelten Datenelements (FS) und des Entwürtelungs-Datenelements (I) über ein lokales Netz zu dem Terminal.

9. Gerät nach Anspruch 8, wobei die Übertragungsmittel einen Datenbus (B) enthalten, der eine asynchrone Verbindung enthält, über die das Entschlüsselungs-Datenelement (I) weitergeleitet wird.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

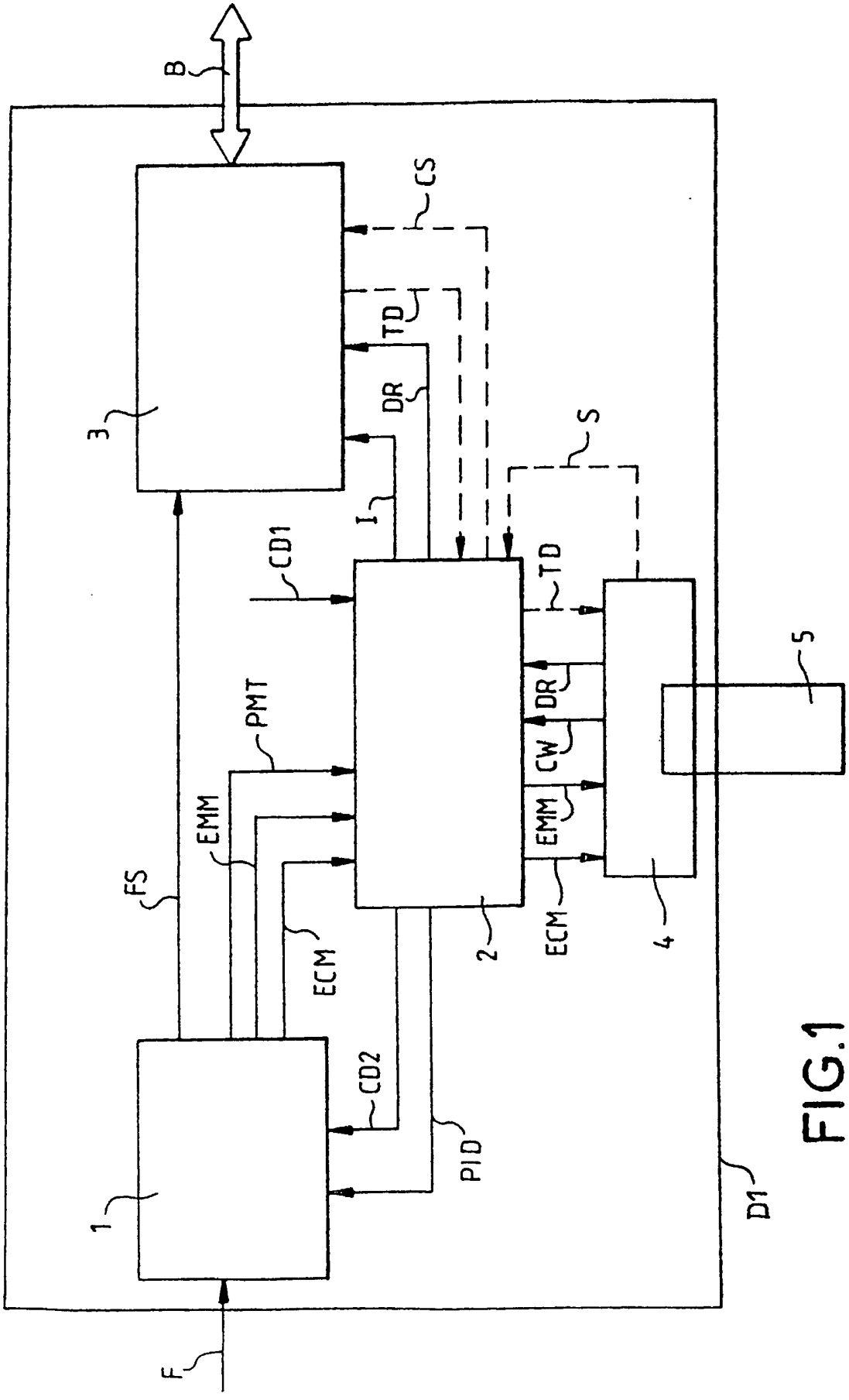

FIG.1

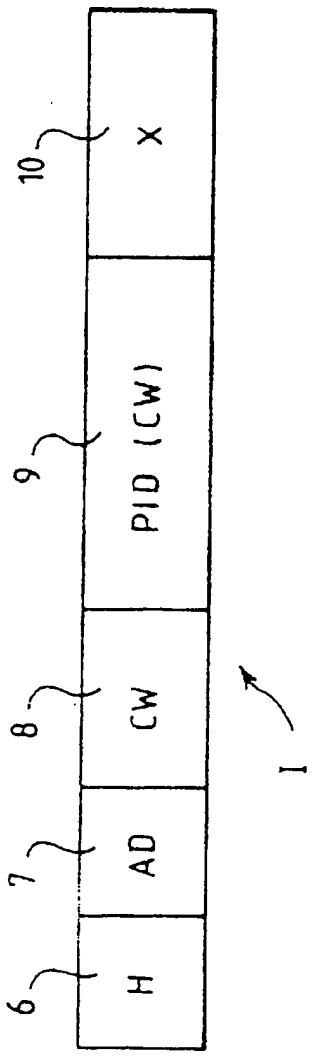

FIG.2

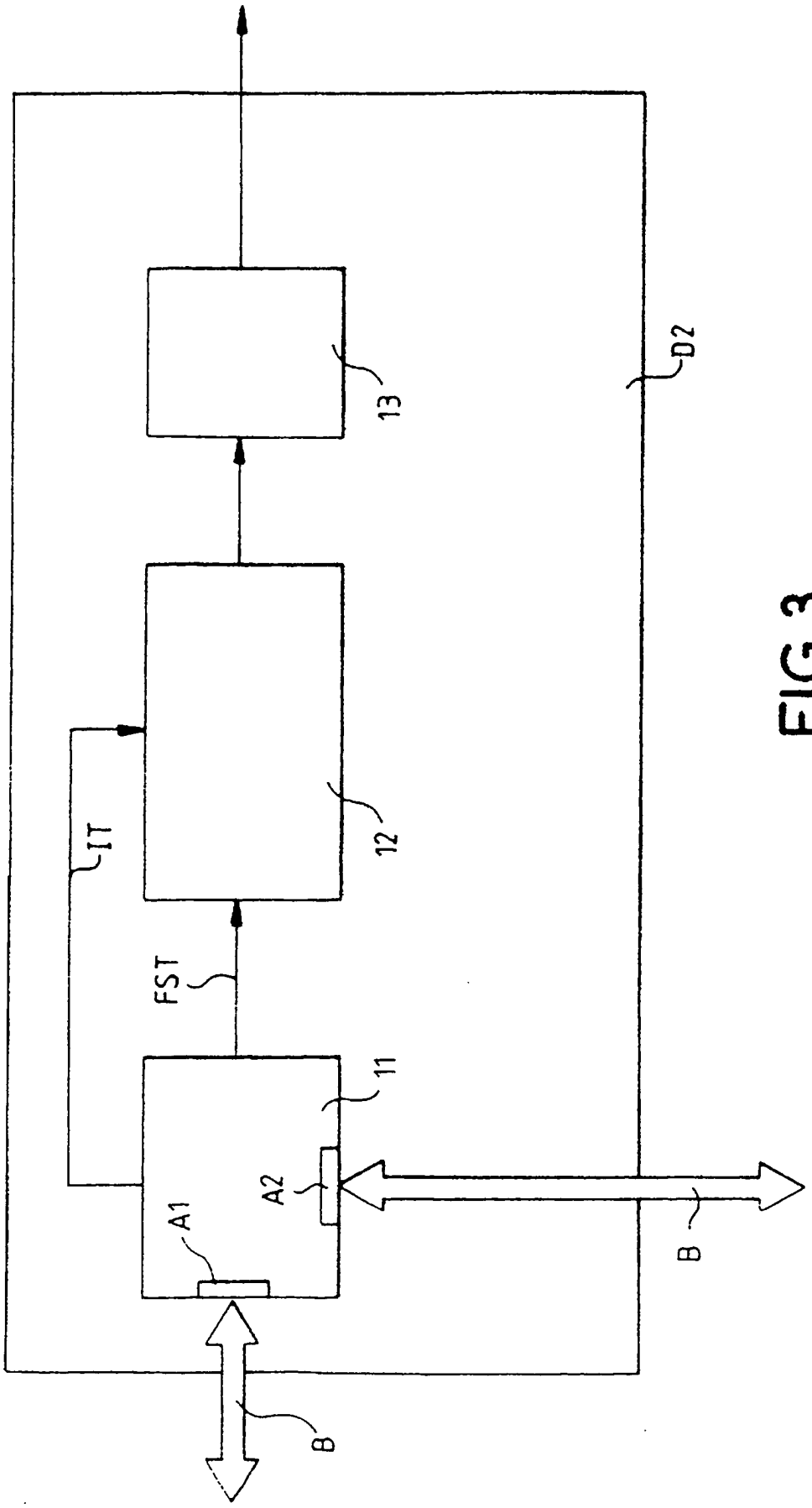

FIG.3