República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0821865-0 B1

(22) Data do Depósito: 31/12/2008

(45) Data de Concessão: 27/10/2020

(54) Título: SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL E PROCEDIMENTO DE MANUSEIO RELACIONADO

(51) Int.Cl.: H04N 21/258; H04N 21/418; H04N 21/4405; H04N 21/442; H04N 21/4623; (...).

(52) CPC: H04N 21/25816; H04N 21/4181; H04N 21/4182; H04N 21/4405; H04N 21/44236; (...).

(30) Prioridade Unionista: 03/01/2008 CN 200810013701.3.

(73) Titular(es): JINAN TAIXIN ELECTRONIC CO., LTD..

(72) Inventor(es): TAO, SHENGHUA.

(86) Pedido PCT: PCT CN2008002145 de 31/12/2008

(87) Publicação PCT: WO 2009/094851 de 06/08/2009

(85) Data do Início da Fase Nacional: 30/06/2010

(57) Resumo: SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL E PROCEDIMENTO DE MANUSEIO RELACIONADO A presente invenção divulga um sistema de acesso condicionado a TV digital e o procedimento de manuseio relacionado. Ela resolve os problemas devidos à segurança, custo e universalidade do sistema de acesso condicionado na versão anterior e apresenta vantagens como a melhora da segurança, a redução do custo e a consolidação da universalidade. O sistema compreende um módulo de autenticação, um módulo de interface inicial de acesso condicionado, no qual o módulo de autenticação se comunica, de forma bidirecional, com o módulo receptor, autentica o módulo receptor, gera um número de ID exclusivo para o receptor e uma informação de autenticação, e registra a informação correspondente no módulo receptor para a base de dados; o módulo de interface inicial de acesso condicionado se comunica de forma bidirecional com a base de dados, lê a informação do receptor a partir da base de dados para criptografar a informação de administração de autenticação do receptor, e distribui a informação mencionada ao módulo receptor em um modo de endereçamento correspondente; o módulo de interface inicial de acesso condicionado compreende o gerador de informação de controle de autenticação correspondente; o módulo receptor (...).

RELATÓRIO DESCRITIVO

SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL E PROCEDIMENTO DE MANUSEIO RELACIONADO

Campo da invenção

[01] A invenção está relacionada a um campo do acesso condicionado a TV digital (incluindo TV a cabo, TV por satélite, TV terrestre e IPTV) e multimídia móvel, e, mais especificamente, a TV digital e um método de uso do mesmo para transmitir e receber dados digitais criptografados.

Histórico da invenção

[02] Um sistema de acesso condicionado (abreviação, AC) é utilizado para controlar o recebimento de dados digitais por um assinante, i.e., o assinante somente pode receber os programas digitais a que tem direito, incluindo áudio, vídeo e dados, de forma que os operadores possam obter lucros dos assinantes pelo controle e administração da concessão de direitos.

[03] No sistema de TV digital, os operadores utilizam um sistema de acesso condicionado para criptografar dados e transmitir programas de TV e somente os assinantes que têm direito podem recebê-los. Além de programas de TV pagos, o sistema AC pode fornecer outros serviços de valor agregado, incluindo vídeo por demanda, serviços de informação e Internet. Desta forma, a receita dos operadores aumenta e se torna uma parte básica e muito importante de um sistema de TV digital.

[04] No entanto, com o rápido desenvolvimento da tecnologia computacional e digital, os sistemas de AC convencionais têm as seguintes desvantagens:

[05] 1 . Baixa segurança

[06] Os sistemas de AC convencionais de TV digital baseiam-se basicamente no padrão DVB da Europa, que foi criado há mais de 10 anos. O seu princípio de funcionamento está descrito abaixo. Um sinal de TV digital criptografado de interface inicial tem um par de chaves secretas que mudam periodicamente, que são chamadas de palavras de controle, ou

abreviadamente de CW. O sistema AC criptografa e transmite a CW a um aparelho de descriptografia de um receptor de TV digital para descriptografia. Desta forma, a CW é obtida e transmitida a um decodificador no qual um fluxo de dados de áudio e vídeo é obtido e reproduzido por um módulo de reprodução.

[07] Na época de desenvolvimento do padrão, a consideração foi focada em como transmitir a CW de forma segura a um receptor, mas não se esperava que uma CW descriptografada pudesse ser difundida e compartilhada pela tecnologia de rede. Por isto, na situação atual com tecnologia de rede altamente desenvolvida, o sistema tem sérias brechas que são utilizadas por piratas e trazem enormes prejuízos aos operadores de TV.

[08] Em geral, o receptor do sistema de AC é um smart card. A descriptografia é salva no smart card. Os dados criptografados são transmitidos para o smart card no qual a CW é obtida. A CW é transmitida para um decodificador por meio de um módulo de AC do receptor. O módulo de AC, como parte separada, é incorporado em uma estrutura de software de uma caixa que se coloca em cima do televisor. A tecnologia tem riscos de segurança porque a CW pode ser interceptada em muitos locais, como mostrado na FIG. 1.

[09] O primeiro local de vazamento é um ponto de comunicação entre o smart card e o receptor.

[010] O segundo local de vazamento é entre o módulo de AC e o decodificador.

[011] O terceiro local de vazamento é a comunicação entre o módulo de AC e a memória (RAM).

[012] Nenhum sistema de AC que tenha um módulo de AC pode evitar o primeiro e o segundo local de vazamento. Obter a CW do terceiro local de vazamento é muito difícil e de custo elevado. Portanto, o primeiro e o segundo local de vazamento apresentam mais problemas. A CW pode ser obtida do primeiro local de vazamento a partir de um dispositivo simples e pode ser obtida

do segundo local de vazamento separando-se o módulo de AC da caixa em cima do televisor. Qualquer um destes métodos é executado com facilidade por tecnologia computacional existente, e resulta no vazamento do AC, mesmo se um código correspondente puder ser encontrado na Internet.

[013] Cada empresa de AC tem dois segredos que são os mais importantes, um é o algoritmo de AC e o outro é o módulo de AC. Com exceção do compartilhamento de rede, a não ser que o algoritmo de AC seja divulgado, o sistema de AC é seguro porque a descriptografia do algoritmo de AC é muito difícil. No entanto, a descriptografia do módulo de AC é muito fácil, o que resulta no colapso do sistema de AC que tem um smart card.

[014] Com base na descriptografia anterior do sistema de AC que tem um smart card, a vida útil do módulo de AC é muito mais longa do que a do algoritmo de AC. Com frequência, o algoritmo foi criptografado muitas vezes, mas o módulo de AC não é mudado. Por isto, na situação atual, com tecnologia de rede altamente desenvolvida, é mais benéfico para os piratas criptografar o módulo de AC.

[015] Para os módulos de AC convencionais, que têm um smart card, a comunicação entre o smart card e a caixa em cima da TV é basicamente fixa, embora haja uma mudança, esta é pequena. No caso de sistemas de AC que emitiram uma grande quantidade de cartões, a mudança é muito difícil. Portanto, mesmo que o fornecedor de AC conheça o local de vazamento da CW, dificilmente há um método para salvar, o que afeta, em grande medida, a competitividade dos operadores de AC. Um sistema de AC convencional com um smart card inclui uma caixa em cima da TV que incorporou muitos módulos de AC correspondentes. O chip da caixa em cima da TV é variável e os módulos de AC são incorporados principalmente pelo fabricante da caixa. Desta forma, os dados de AC são facilmente difundidos e vazados. Mesmo que não ocorra vazamento, um hacker comum pode analisar, com sucesso, o módulo de AC a partir da memória do programa da caixa em cima da TV. Uma vez analisados,

os dados podem ser usados por um longo tempo. Portanto, o smart card do sistema de AC convencional tem sérios riscos de segurança.

[016] 2. Universalidade precária

[017] Para melhorar o índice de segurança, o sistema de AC convencional tem muita privacidade. Cada fornecedor de AC criptografa os seus próprios dados conforme as possibilidades que tem. Desta forma, o fabricante da caixa em cima da TV dificilmente pode integrar muitos módulos de AC na caixa, o que torna esta caixa não universal.

[018] Além disto, é muito difícil para os fornecedores de AC fornecer um sistema de AC para cada operador de AC. O algoritmo de AC fornecido por um fornecedor de AC é sempre o mesmo, quando o sistema de AC usado por um operador é descriptografado, todos os outros operadores serão afetados.

[019] 3. Custo elevado

[020] No receptor convencional de AC, uma unidade de controle de descriptografia compreende um circuito de interface de smart card, um dispositivo leitor do smart card e um smart card especial, o que aumenta, em grande medida, o custo de recepção de TV digital, desperdiça recursos e limita a popularização da TV digital.

[021] Em vista dos problemas descritos acima, um dos objetivos da invenção é fornecer um sistema de acesso condicionado à TV digital que tenha elevada segurança, baixo custo e boa universalidade, e um método de utilização deste para transmitir e receber dados digitais criptografados.

[022] Para atingir os objetivos acima, a invenção fornece um sistema de acesso condicionado a TV que compreende um módulo de autenticação, um módulo de interface inicial de acesso condicionado e um módulo receptor, no qual o módulo de autenticação se comunica de forma bidirecional com o módulo receptor, o qual autentica, para gerar um número de ID e informação de autenticação exclusivos, sendo que o número de ID e a informação de autenticação são gravados em uma base de dados; e o módulo de interface inicial de acesso

condicionado se comunica de forma bidirecional com a base de dados, coleta informações do módulo receptor a partir da base de dados, criptografa a mensagem de administração de diretos do módulo receptor, e transmite a mensagem de administração de direitos ao módulo receptor por um modo de endereçamento; o módulo de interface inicial de acesso condicionado compreende ainda um gerador de mensagens de controle de direitos e se conecta a uma porta de download externa; e o módulo receptor recebe um programa codificado com a ajuda do número de ID e da informação de autenticação.

[023] Nesta classe de materialização, o módulo de autenticação compreende um chip principal do receptor, um chip de segurança e um chip de memória, todos os quais cooperam com a base de dados e têm uma identidade exclusiva e uma área de dados que pode ser escrita uma vez e não pode ser apagada; o chip principal tem uma ROM que compreende a área de dados; e, após a autenticação, o número de ID exclusivo e a informação de autenticação são salvos em um hardware do receptor e não podem ser copiados.

[024] Nesta classe de materialização, o módulo de interface inicial de acesso condicionado compreende um codificador, o gerador de mensagens de controle de direitos, um gerador de mensagens de administração de direitos e um sistema de administração de assinantes; o codificador recebe, processa e transmite áudio, vídeo, dados e informação criptografada gerada pelo gerador de mensagens de controle de direitos e pelo gerador de mensagens de administração de direitos; o sistema de administração de assinantes controla o gerador de mensagens de administração de direitos e se comunica, de forma bidirecional, com a base de dados; e a base de dados se comunica, de forma bidirecional, com o gerador de mensagens de administração de direitos.

[025] Nesta classe de materialização, o módulo receptor compreende um módulo de demultiplexação, CPU, um decodificador, um módulo de reprodução, um módulo de controle de decodificação e um módulo de memória; o módulo de

demultiplexação recebe um fluxo de transmissão criptografado para receber dois fluxos de dados, um é um fluxo de dados de áudio e vídeo codificados, que é transmitido por um canal de dados ao decodificador para decodificação, o outro é mensagem de controle de direitos e mensagem de administração de direitos; a mensagem de controle de direitos e a mensagem de administração de direitos são processadas pela CPU e transmitidas ao módulo de controle de decodificação para produzir uma palavra de controle; o decodificador utiliza a palavra de controle para descriptografar o fluxo de dados de áudio e vídeo criptografado; e o fluxo de áudio e vídeo descriptografado resultante é transmitido ao módulo de reprodução para reprodução.

[026] O sistema de acesso condicionado pode facilmente atualizar o algoritmo do sistema de acesso condicionado do módulo do receptor e o módulo da interface inicial de acesso condicionado. Pela atualização periódica do algoritmo do sistema de acesso condicionado, a segurança do sistema foi melhorada de forma significativa.

[027] Um método de utilização do sistema de acesso condicionado à digital para a transmissão e recepção de dados digitais criptografados compreende

[028] a) processo de autenticação: o passo que focaliza a autenticação sistêmica do receptor, mediante a produção, o exame de compatibilidade entre os hardwares e o registro de informações efetivas do receptor, e compreendendo: combinação de um chip principal com um chip de segurança por um algoritmo e registro da informação de cada um e da informação comum; combinação do chip principal com um chip de memória por um algoritmo e registro da informação de cada um e da memória comum; combinação do chip de segurança com o chip de memória por um algoritmo e registro da informação de cada um e a informação comum; transmissão de toda a informação pelo receptor para um servidor de autenticação onde os dados são examinados; registro dos dados examinados com sucesso para a base de dados e alocação do número de ID exclusivo e um código de segurança para o receptor, o número

da ID funcionando como base para endereçamento condicional, e o código de segurança funcionando como base para verificação da autenticidade do receptor;

[029] b) processo de interface inicial do acesso condicionado: investigação do número da ID a partir da base de dados por um sistema de administração de assinantes, após receber instruções de um operador, se existir, transmissão da instrução ao módulo de interface inicial de acesso condicionado, geração de dados de acordo com as informações do receptor como uma chave secreta de mensagem de administração de direitos criptografada, geração de mensagem de administração de diretos criptografada por um gerador de mensagem de administração de direitos, e entrada em uma rede de TV digital por meio de um codificador, enquanto gera mensagem de controle de direitos por um gerador de mensagens de controle de direitos e entrada na rede de TV digital;

[030] c) processo de interface final do acesso condicionado: demultiplexação de sinais digitais pelo receptor para gerar dados codificados de áudio e vídeo que são transmitidos diretamente para o decodificador e a mensagem de controle de direitos e mensagem de administração de direitos, filtrando a mensagem de controle de direitos em uma memória para gerar informações efetivas e uma mensagem de direitos; e

[031] d) atualização do algoritmo do sistema de acesso condicionado: quando um algoritmo do sistema de acesso condicionado em uso é descriptografado ou precisa ser atualizado devido a considerações de segurança, o processo é executado, compreendendo: transmissão de um novo algoritmo do sistema de acesso condicionado por meio de um multiplexador, o decodificador e um modulador do módulo de interface inicial de acesso condicional para uma rede de TV digital, recebimento do novo algoritmo do sistema de acesso condicionado, e atualização de um algoritmo antigo do sistema de acesso condicionado com o novo algoritmo do sistema de acesso condicionado.

[032] Nesta classe de materialização, no passo c), o receptor primeiramente examina a compatibilidade do chip principal com o chip de segurança, a compatibilidade do chip principal com o chip de memória, e a compatibilidade do chip de segurança com o chip de memória; mediante o sucesso, uma mensagem efetiva de administração é filtrada de acordo com a ID do receptor, e uma chave secreta da mensagem de administração de direitos é calculada de acordo com a informação compatibilizada; a mensagem de administração de direitos é descriptografada para gerar diretos para criptografar a mensagem de controle de direitos e uma outra chave secreta; a mensagem de controle de direitos é descriptografada para gerar uma palavra de controle que é transmitida ao decodificador; o decodificador decodifica os dados de áudio e vídeo de acordo com a palavra de controle; os dados de áudio e vídeo decodificados são transmitidos ao módulo de reprodução para reprodução.

[033] Nesta classe de materialização, no passo d), o novo algoritmo do sistema de acesso condicionado não atualiza o antigo algoritmo do sistema de acesso condicionado em uso, mas o salva no receptor, de forma que o receptor tem dois algoritmos do sistema de acesso condicionado; o receptor seleciona um algoritmo do sistema de acesso condicionado dos dois tipos de algoritmo do sistema de acesso condicionado, de acordo com o algoritmo do sistema de acesso condicionado usado pelo módulo de interface inicial de acesso condicionado para receber os dados de áudio e vídeo codificados. Além disso, para evitar o uso ilegal do algoritmo do sistema de acesso condicionado, a legalidade do módulo receptor é examinada para que um módulo receptor ilegal não possa utilizar o algoritmo atualizado do sistema de acesso condicionado.

[034] O padrão convencional de DVB foi utilizado por mais de dez anos, e o equipamento de interface inicial e final ocupa uma grande fatia do mercado, modificar o padrão significa atualizar o equipamento, pelo que se pagará um preço elevado. A invenção soluciona os riscos de segurança do acesso condicionado convencional sob o padrão de DVB existente, e o sistema tem boa

universalidade. Na invenção, o módulo de AC e os programas do aplicativo estão integrados em um módulo, o algoritmo do AC e o módulo do AC não estão separados, desta forma, nenhuma informação sobre a CW pode ser obtida de fora do módulo receptor, o que garante a segurança do sistema. Além disso, o sistema não envolve smart card, e com isto, economiza-se o circuito da interface do smart card, um dispositivo leitor de smart card e um smart card especial e os programas de AC são simplificados, o que reduz, em grande medida, o custo do receptor.

[035] As vantagens da invenção estão resumidas abaixo. O sistema não envolve smart card, e com isto, economiza-se o circuito da interface do smart card, um dispositivo leitor de smart card e um smart card especial e os programas de AC são simplificados, o que reduz, em grande medida, o custo do receptor. A invenção soluciona totalmente o local de vazamento 1 da CW da versão anterior, da interface inicial å interface final, e como o módulo de AC e os programas dos aplicativos estão integrados, não há local de vazamento 2 da CW da versão anterior. Embora a CW possa ser compartilhada por meio de fraude de empresas de desenvolvimento de chips, elas assumem grandes riscos de negócios e legais. Na invenção, para obter a CW do local de vazamento 3 da versão anterior significa descriptografar todos os programas do módulo receptor, portanto não há qualquer valor de negócio. Como quase todos os chips existentes suportam a implementação de um código de download, o algoritmo de criptografia do sistema de acesso condicionado pode ser atualizado por um novo código dinâmico transmitido a partir da interface inicial de acesso condicionado. Quando o tempo de atualização é menor do que o tempo de descriptografia, a descriptografia do algoritmo de criptografia se torna insignificante, o que melhora a segurança do sistema. Além disso, como o módulo receptor suporta a implementação de um código de download em diferentes regiões, o receptor que tem o mesmo software e hardware pode fazer downloads de forma seletiva e implementar programas de acordo com diferentes

operadores de TV digital, o que melhora a universalidade entre o receptor e o sistema de acesso condicionado.

[036] Desta forma, a invenção supera as desvantagens do sistema de acesso condicionado convencional, como baixa segurança, elevado custo e universalidade precária, e fornece um sistema de acesso condicionado a TV digital com elevada segurança, baixo custo e boa universalidade, estrutura simples e prática conveniente.

[037] A FIG. 1 é um diagrama esquemático de vazamento de segurança do sistema de acesso condicionado que tem um smart card da versão anterior;

[038] A FIG. 2 é um fluxograma geral de um sistema de acesso condicionado, de acordo com uma materialização da invenção;

[039] A FIG. 3 é um fluxograma da autenticação, de acordo com uma materialização da invenção;

[040] A FIG. 4 é um fluxograma de um módulo de interface inicial de acesso condicionado, de acordo um uma materialização da invenção;

[041] A FIG. 5 é um fluxograma de um módulo receptor, de acordo com uma materialização da invenção; e

[042] A FIG. 6 é um fluxograma detalhado do processador de acesso condicionado, de acordo com uma materialização da invenção;

[043] Legenda: 1. Base de dados; 2. Módulo de interface inicial de acesso condicionado; 3. Módulo de autenticação; 4. Módulo receptor; 5. Chip principal; 6. Chip de segurança; 7. Chip de memória; 8. Codificador; 9. Gerador de mensagens de controle de direitos; 10. Gerador de mensagens de administração de direitos; 11. Sistema de administração de assinantes; 12. Decodificador; 13. Módulo de demultiplexação; 14. CPU; 15. Módulo de reprodução; 16. Módulo de controle de descriptografia; 17. Módulo de memória.

[044] A invenção está descrita abaixo, neste documento, com referência a desenhos que acompanham.

[045] Como mostrado na FIG. 2, um fluxograma geral de um sistema de acesso condicionado. O sistema compreende um módulo de autenticação 3, um módulo de interface inicial de acesso condicionado 2, e um módulo receptor 4. O módulo de autenticação 3 se comunica de forma bidirecional com o módulo receptor 4, o qual autentica, para gerar um número de ID exclusivo e informação de autenticação (A1A2). O número de ID e a informação de autenticação do módulo receptor 4 são registrados em uma base de dados 1 (A3). O módulo de interface inicial de acesso condicionado 2 se comunica de forma bidirecional com a base de dados 1, coleta informação do módulo receptor a partir da base de dados 1, criptografa a mensagem de administração de direitos e o módulo receptor (A1*-A2*), e transmite a mensagem de administração de direitos criptografada ao módulo receptor 4 por meio de um modo de endereçamento (A3*); o módulo de interface inicial de acesso condicionado 2 ainda compreende um gerador de mensagens de controle de direitos; e o módulo receptor 4 recebe um programa codificado com a ajuda do número de ID, da informação de autenticação e dos softwares. O módulo receptor pode atualizar o algoritmo de acesso condicionado de acordo com o módulo de interface inicial de acesso condicionado

[046] Conforme mostrado na FIG. 3, um fluxograma de autenticação. O processo compreende a combinação do chip principal 5 com um chip de memória 7 por um algoritmo e registro da informação de cada um e a informação comum (B1, B7); combinação do chip principal 5 com um chip de segurança 6 por um algoritmo e registro da informação de cada um e a informação comum (B2, B8); combinação do chip de segurança 6 com o chip de memória 7 por um algoritmo e registro da informação de cada um e a informação comum (B1, B2); transmissão de toda a informação pelo receptor a um servidor de autenticação (B3) onde os dados são examinados; registro dos dados examinados com sucesso na base de dados (B4) e alocando o número de ID exclusivo {ID} e um código de segurança (B5-B6) ao receptor. O número de ID e o código de segurança estão criptografados e salvos no chip de memória 7 e no chip de

segurança 6 (B7, B8). As funções do número de ID como base para o endereçamento condicionado, e as funções do código de segurança como base para verificação da autenticidade do receptor.

[047] Conforme mostrado na FIG. 4, um fluxograma de um módulo de interface inicial de acesso condicionado 2. O processo compreende a investigação do número de ID a partir da base de dados por um sistema de administração de assinantes 11 após receber instruções de um operador (C21), se existir, transmissão da instrução ao módulo de interface inicial de acesso condicionado 2 (C22), geração de dados de acordo com a informação do receptor como chave secreta da mensagem de administração de direitos criptografada (C23), geração de mensagem de administração de direitos por um gerador de mensagens de administração de direitos 10, e entrada em uma rede de TV digital (C4) junto com dados de áudio e vídeo (Cl) por meio de um codificador 8, e enquanto isso, a geração de uma mensagem de controle de direitos por um gerador de mensagens de controle de direitos 9 e entrada em uma rede de TV digital (C3).

[048] Conforme mostrado na FIG. 5, um fluxograma de um módulo receptor. O processo compreende a demultiplexação de sinais digitais (DO) por um módulo de demultiplexação 13 do receptor para gerar dados de áudio e vídeo que são codificados pelo codificador 8 e transmitidos diretamente a um módulo de controle de decodificação 16 (Dl) e mensagem de controle de direitos e mensagem de administração de direitos que são transmitidos à CPU 14 conectada ao chip de memória 7 e o chip de segurança 6, filtração da mensagem de controle de direitos em uma memória para gerar mensagem de direitos (D2-D5). Após a mensagem de direitos e a chave secreta para descriptografar a mensagem de controle de direitos terem sido obtidos, a mensagem de controle de direitos é descriptografada para produzir uma palavra de controle que é transmitida a um decodificador 12 (D6). O decodificador 12 decodifica dados de áudio e vídeo de acordo com a palavra de controle, e os dados de áudio e vídeo

decodificados são transmitidos para um módulo de reprodução 15 para reprodução (D7-D8).

[049] Conforme mostrado na FIG. 6, um fluxograma detalhado de um processador de acesso condicionado pelo qual uma mensagem de controle de direitos efetiva é filtrada e decodificada em um módulo de memória 17. O processo compreende a comunicação da 14 de forma bidirecional com o módulo de memória 17, o chip de segurança 6, e o chip de memória 7 respectivamente, exame da compatibilidade do chip principal 5 com o chip de segurança 6, a compatibilidade do chip principal 5 com o chip de memória 7, e a compatibilidade do chip de segurança 6 com o chip de memória 5(E1-E2), se incompatível, encerrar o trabalho, se compatível, filtrar a mensagem de administração de direitos efetiva (E3) de acordo com a identidade do receptor, cálculo de uma chave secreta da mensagem de administração de direitos de acordo com a informação compatibilizada (E4), e a descriptografia da mensagem de administração de direitos para processamento adicional (E5).

[050] Um método de utilização do sistema de acesso condicionado à TV digital para a transmissão e recepção de dados digitais criptografados compreendendo

[051] a) processo de autenticação: o passo focaliza a autenticação sistêmica do receptor, mediante a produção, o exame de compatibilidade entre os hardwares e o registro de informações efetivas do receptor, compreendendo: combinação do chip principal com o chip de segurança por um algoritmo e registro da informação de cada um e da informação comum; combinação do chip principal com o chip de memória por um algoritmo e registro da informação de cada um e da memória comum; combinação do chip de segurança com o chip de memória por um algoritmo e registro da informação de cada um e a informação comum; transmissão de toda a informação pelo receptor para um servidor de autenticação onde os dados são examinados; registro dos dados examinados com sucesso para a base de dados e alocação do número de ID exclusivo e do código de segurança para o receptor, o número da ID funcionando

como base para endereçamento condicional, e o código de segurança funcionando como base para verificação da autenticidade do receptor;

[052] b) processo de interface inicial do acesso condicionado: investigação do número da ID a partir da base de dados pelo sistema de administração de assinantes, após receber instruções de um operador, se existir, transmissão da instrução ao módulo de interface inicial de acesso condicionado, geração de dados de acordo com as informações do receptor como uma chave secreta de mensagem de administração de direitos criptografada, geração de mensagem de administração de diretos criptografada por um gerador de mensagem de administração de direitos, e entrada em uma rede de TV digital por meio do codificador, enquanto gera mensagem de controle de direitos pelo gerador de mensagens de controle de direitos e entrada na rede de TV digital;

[053] c) processo de interface final do acesso condicionado: demultiplexação de sinais digitais pelo receptor para gerar dados codificados de áudio e vídeo que são transmitidos diretamente para o decodificador e a mensagem de controle de direitos e mensagem de administração de direitos, filtrando a mensagem de controle de direitos em uma memória para gerar informações efetivas e uma mensagem de direitos; e

[054] d) atualização do algoritmo do sistema de acesso condicionado: quando um algoritmo do sistema de acesso condicionado em uso é descriptografado ou precisa ser atualizado devido a considerações de segurança, o processo é executado, compreendendo: transmissão de um novo algoritmo do sistema de acesso condicionado por meio de um multiplexador, o decodificador e um modulador do módulo de interface inicial de acesso condicional para uma rede de TV digital, recebimento do novo algoritmo do sistema de acesso condicionado, e atualização de um algoritmo antigo do sistema de acesso condicionado com o novo algoritmo do sistema de acesso condicionado.

[055] Especificamente, no passo c), o receptor primeiramente examina a compatibilidade do chip principal com o chip de segurança, a compatibilidade do

chip principal com o chip de memória, e a compatibilidade do chip de segurança com o chip de memória; mediante o sucesso, uma mensagem efetiva de administração é filtrada de acordo com a ID do receptor, e uma chave secreta da mensagem de administração de direitos é calculada de acordo com a informação compatibilizada; a mensagem de administração de direitos é descriptografada para gerar diretos para criptografar a mensagem de controle de direitos e uma outra chave secreta; a mensagem de controle de direitos é descriptografada para gerar uma palavra de controle que é transmitida ao decodificador; o decodificador decodifica os dados de áudio e vídeo de acordo com a palavra de controle; os dados de áudio e vídeo decodificados são transmitidos ao módulo de reprodução para reprodução.

[056] Especificamente, no passo d), o novo algoritmo do sistema de acesso condicionado não atualiza o antigo algoritmo do sistema de acesso condicionado em uso, mas o salvou no receptor, de forma que o receptor tem dois algoritmos do sistema de acesso condicionado; o receptor seleciona um algoritmo do sistema de acesso condicionado dos dois tipos de algoritmo do sistema de acesso condicionado, de acordo com o algoritmo do sistema de acesso condicionado usado pelo módulo de interface inicial de acesso condicionado para receber os dados de áudio e vídeo codificados. Além disso, para evitar o uso ilegal do algoritmo do sistema de acesso condicionado, a legalidade do módulo receptor é examinada para que um módulo receptor ilegal não possa utilizar o algoritmo atualizado do sistema de acesso condicionado.

[057] O algoritmo do sistema de acesso condicionado da invenção pode ser qualquer algoritmo alinhado ao padrão DVB.

[058] Aqueles não descritos em detalhe na invenção são divulgados pela versão anterior.

REIVINDICAÇÕES

1. SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL que compreende um servidor de autenticação, um módulo de interface inicial de acesso condicionado e um módulo receptor, caracterizado pelo fato de que

o dito servidor de autenticação, ao ser produzido, se comunica de forma bidirecional com o dito módulo receptor e autentica o dito módulo receptor para gerar um número de ID exclusivo do módulo receptor e informação de autenticação do módulo receptor, o dito número de ID e a dita informação de autenticação sendo registrados em uma base de dados, o dito número de ID funcionando como base para endereçamento condicional, em que o módulo receptor compreende um chip principal, um chip de segurança, e um chip de memória, o dito chip principal sendo combinado com o dito chip de segurança por um algoritmo, e a informação de cada um e da memória comum são registradas; dito chip principal é combinado com o dito chip de memória por um algoritmo, e a informação de cada um e a informação comum são registradas; o dito chip de segurança sendo combinado com o dito chip de memória por um algoritmo, e a informação de cada um e a informação comum sendo registradas;

o dito módulo de acesso de interface inicial condicionado se comunica de forma bidirecional com a dita base de dados, coleta a informação de autenticação do dito módulo receptor a partir da dita base de dados, criptografa mensagem de administração de direito do dito módulo receptor, e transmite a dita mensagem de administração de diretos criptografada com a informação de autenticação ao dito módulo receptor por meio de um modo de endereçamento; o dito módulo de interface inicial de acesso condicionado compreendendo ainda um gerador de mensagem de controle de direitos e se conectando a uma porta de download externa; e

o dito módulo receptor recebe um programa codificado com a ajuda do dito número de ID e a dita informação de autenticação, em que o dito receptor

primeiramente examina a compatibilidade do chip principal com o chip de segurança, a compatibilidade do chip principal com o chip de memória, e a compatibilidade do chip de segurança com o chip de memória; mediante o sucesso, uma mensagem efetiva de administração é filtrada de acordo com a ID do dito receptor, e uma chave secreta da mensagem de administração de direitos é calculada de acordo com as informações compatibilizadas; a dita mensagem de administração de direitos sendo descriptografada, e processos correspondentes sendo realizados de acordo com o resultado da descriptografia.

2. SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL, de acordo com a reivindicação 1, **caracterizado** por cada um dos ditos chip principal, chip de segurança e chip de memória cooperar com a dita base de dados e ter uma identidade exclusiva e uma área de dados que está escrita somente uma vez e não pode ser apagada; o dito chip principal ter uma ROM que compreende a dita área de dados; e, após a identificação, o dito número de ID exclusivo e a informação de autenticação serem salvos em um hardware do dito receptor e não poderem ser copiados.

3. SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito módulo de interface inicial de acesso compreende um codificador, o dito gerador de mensagens de controle de direitos, um gerador de mensagens de administração de direitos, e um sistema de administração de assinantes; o dito codificador recebe, processa e transmite dados de áudio e vídeo e informação codificada gerada pelo dito gerador de mensagens de controle de direitos e o dito gerador de mensagens de administração de direitos; o dito sistema de administração de assinantes controla o dito gerador de mensagens de direitos e se comunica, de forma bidirecional, com o dito gerador de mensagens de administração de direitos.

4. SISTEMA DE ACESSO CONDICIONADO A TV DIGITAL, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito módulo receptor

compreende um módulo de demultiplexação, CPU, um decodificador, um módulo de reprodução, um módulo de controle de decodificação, e um módulo de memória; o dito módulo de demultiplexação recebe um fluxo de transmissão criptografado e obtém dois fluxos de dados, sendo um fluxo de dados de áudio e vídeo codificado que é transmitido por um canal de dados ao dito decodificador para decodificação, e o outro é uma mensagem de controle de direitos e uma mensagem de administração de direitos; a dita mensagem de controle de direitos e a dita mensagem de administração de direitos sendo processadas pela dita CPU e transmitidas ao dito módulo de controle de decodificação para produzir uma palavra de controle; o dito decodificador utilizando a dita palavra de controle para descriptografar o dito fluxo de dados de áudio e vídeo codificado dito; e o fluxo de dados de áudio e vídeo descriptografado resultante é transmitido ao módulo de reprodução dito para reprodução.

5. MÉTODO DE UTILIZAÇÃO DO SISTEMA DE ACESSO CONDICIONADO À TV DIGITAL conforme descrito na reivindicação 1 para a transmissão e recepção de dados digitais criptografados, **caracterizado por** compreender:

a) processo de autenticação: o passo focaliza a autenticação sistêmica do dito receptor, mediante a produção, o exame de compatibilidade entre os hardwares e o registro de informações efetivas do dito receptor, compreendendo: combinação de um chip principal com um chip de segurança por um algoritmo e registro da informação de cada um e da informação comum; combinação do dito chip principal com um chip de memória por um algoritmo e registro da informação de cada um e da memória comum; combinação do dito chip de segurança com o dito chip de memória por um algoritmo e registro da informação de cada um e a informação comum; transmissão de toda a informação pelo dito receptor dito para um servidor de autenticação onde os dados são examinados; registro dos dados examinados com sucesso na dita base de dados e alocação do dito

número de ID exclusivo e um código de segurança para o dito receptor, o dito número da ID funcionando como base para endereçamento condicional, e o dito código de segurança funcionando como base para a verificação da autenticidade da máquina;

b) processo de interface inicial do acesso condicionado: investigação do dito número da ID a partir da dita base de dados por um sistema de administração de assinantes, após receber instruções de um operador, se existir, transmissão da instrução ao dito módulo de interface inicial de acesso condicionado, geração de dados de acordo com as informações do dito receptor como uma chave secreta de mensagem de administração de direitos criptografada, geração de mensagem de administração de diretos criptografada por um gerador de mensagem de administração de direitos, e entrada em uma rede de TV digital por meio do dito codificador, enquanto gera mensagem de controle de direitos por um gerador de mensagens de controle de direitos e entrada na rede de TV digital;

c) processo de interface inicial do acesso condicionado: demultiplexação de sinais digitais pelo dito receptor para gerar dados codificados de áudio e vídeo que são diretamente transmitidos para o dito decodificador e a mensagem de controle de direitos e mensagem de administração de direitos, filtrando a dita mensagem de controle de direitos em uma memória para gerar informações efetivas e uma mensagem de direitos; o dito receptor examinar, em primeiro lugar, a compatibilidade do dito chip principal com o dito chip de segurança, a compatibilidade do dito chip principal com o dito chip de memória, e a compatibilidade do dito chip de segurança com o dito chip de memória; mediante o sucesso, uma mensagem de administração de direitos efetiva é filtrada de acordo com a ID do dito receptor, e uma chave secreta da dita mensagem de administração de direitos ser calculada de acordo com as informações compatibilizadas; a dita mensagem de administração de direitos ser descriptografada para gerar um direito para descriptografar a dita mensagem de

controle de direitos e outra chave secreta; a dita mensagem de controle de direitos ser descriptografada para gerar uma palavra de controle que é transmitida ao dito decodificador; o dito decodificador decodificar os dados de áudio e vídeo de acordo com a dita palavra de controle; os ditos dados de áudio e vídeo decodificados serem transmitidos ao dito módulo de reprodução para reprodução;

d) atualização do algoritmo do sistema de acesso condicionado: quando um algoritmo do sistema de acesso condicionado em uso é descriptografado ou precisa ser atualizado devido a considerações de segurança, o processo é executado, compreendendo: transmissão de um novo algoritmo do sistema de acesso condicionado por meio de um multiplexador, o dito decodificador, e um modulador do dito módulo de interface inicial de acesso condicional para uma rede de TV digital, recebimento do dito novo algoritmo do sistema de acesso condicionado, pelo módulo receptor dito e atualização de um algoritmo antigo do sistema de acesso condicionado com o dito novo algoritmo do sistema de acesso condicionado.

6. MÉTODO DE UTILIZAÇÃO DO SISTEMA DE ACESSO CONDICIONADO À TV DIGITAL, de acordo com a reivindicação 5, **caracterizado por** conter no passo d), o dito novo algoritmo do sistema de acesso condicionado não atualizar o antigo algoritmo do sistema de acesso condicionado em uso, mas ser salvo no dito receptor de forma que o dito receptor tenha dois tipos de algoritmo de sistema de acesso condicionado; o dito receptor selecionar um algoritmo de sistema de acesso condicionado dos dois tipos de algoritmo de sistema de acesso condicionado de acordo com o algoritmo do sistema de acesso condicionado usado pelo módulo de interface inicial de acesso condicionado dito para receber dados de áudio e vídeo codificado.

7. MÉTODO DE UTILIZAÇÃO DO SISTEMA DE ACESSO CONDICIONADO À TV DIGITAL, de acordo com a reivindicação 5,

caracterizado por conter no passo d), evitar que o dito algoritmo do sistema de acesso condicionado seja utilizado de forma ilegal, a legalidade do dito módulo receptor sendo examinada de forma que o módulo do receptor ilegal não possa utilizar o algoritmo do sistema de acesso condicionado atualizado.

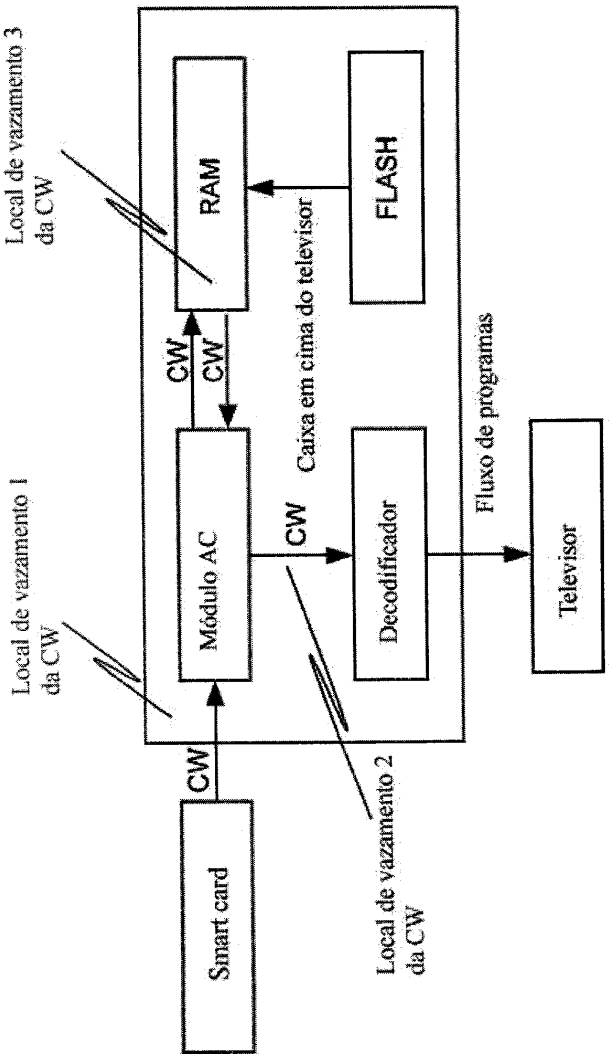


Fig. 1 (Versão anterior)

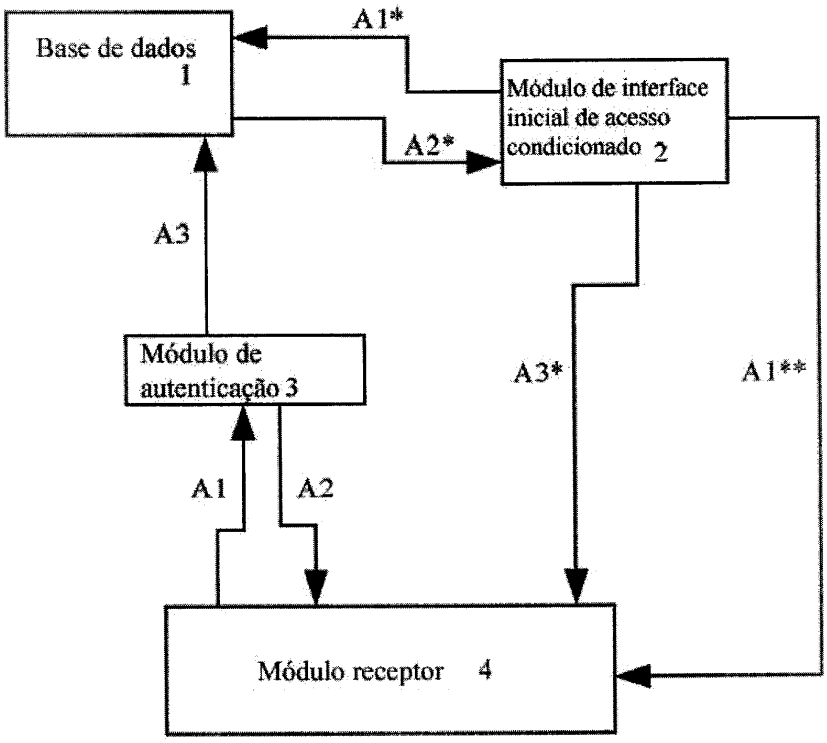

Base de dados
1
A1*
Módulo de interface
inicial de acesso
condicionado 2
A2*
A3
Módulo de
autenticação 3
A3*
A1**
A1
A2
Módulo receptor 4

Fig. 2

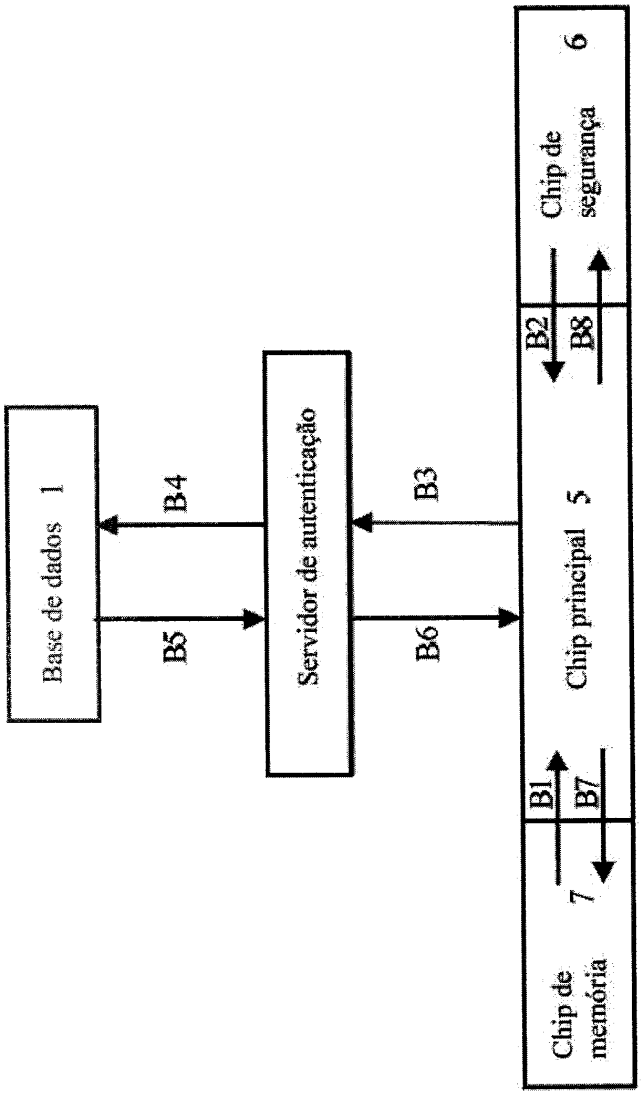

Base de dados 1
B4
B5
Servidor de autenticação
B3
B6
Chip principal 5
B2
B8
Chip de segurança 6
B1
B7
Chip de memória 7

Fig. 3

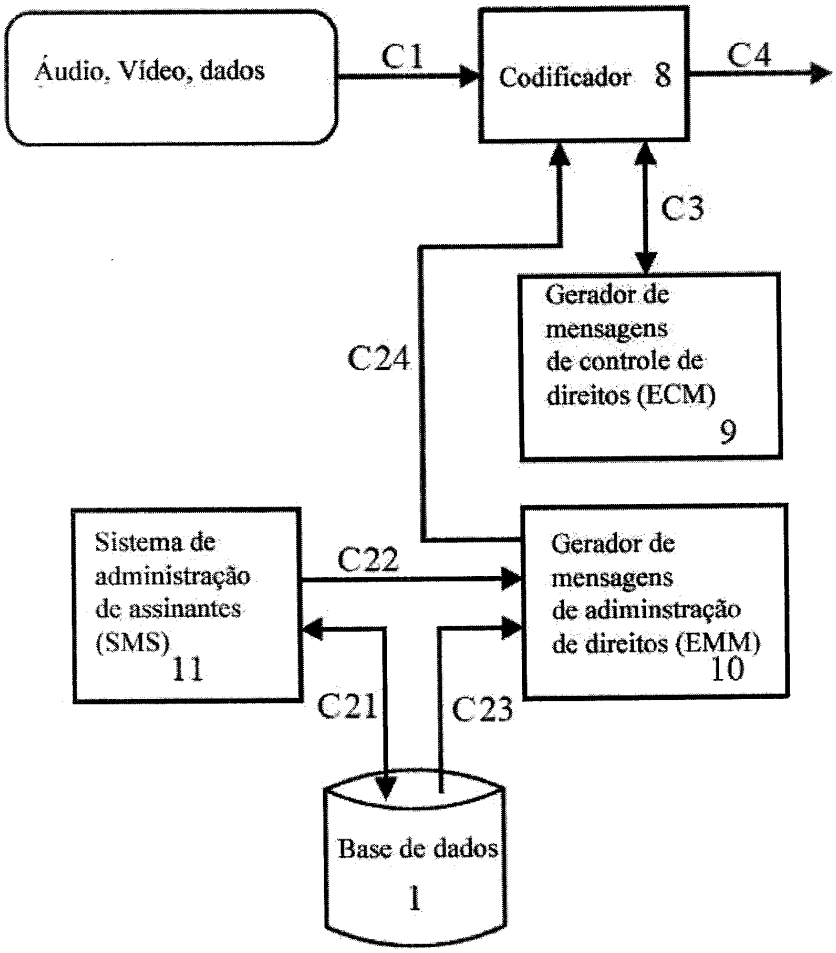

Áudio, Vídeo, dados
C1
Codificador 8
C4
C3
C24
Gerador de mensagens de controle de direitos (ECM) 9
Sistema de administração de assinantes (SMS) 11
C22
Gerador de mensagens de adiminstração de direitos (EMM) 10
C21
C23
Base de dados 1

Fig. 4

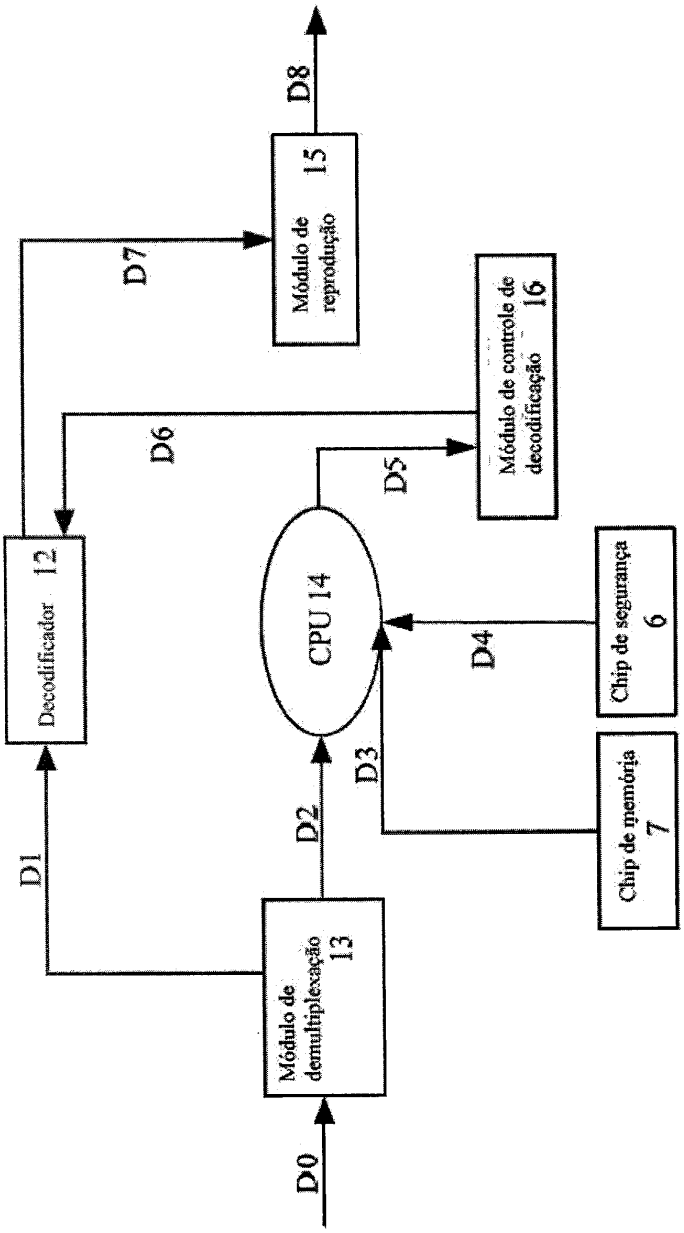

D0
Módulo de demultiplexação 13
D1
D2
D3
D4
D5
D6
D7
D8
Decodificador 12
CPU 14
Chip de memória 7
Chip de segurança 6
Módulo de controle de decodificação 16
Módulo de reprodução 15

FIG. 5

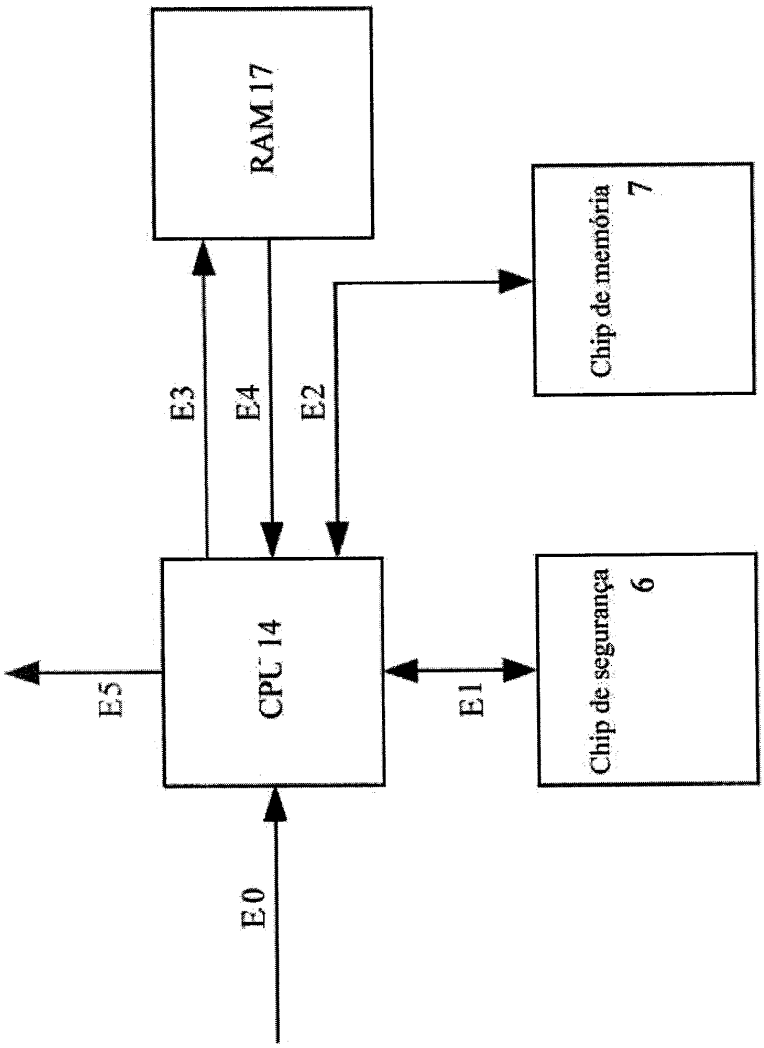

RAM 17
Chip de memória 7
E3
E4
E2
E5
CPU 14
E1
Chip de segurança 6
E0

FIG. 6