**República Federativa do Brasil**
Ministério da Indústria, Comércio Exterior
e Serviços
Instituto Nacional da Propriedade Industrial

**(11) PI 0407202-2 B1**

**(22) Data do Depósito:** 30/01/2004

**(45) Data de Concessão:** 11/07/2017

**(54) Título:** SISTEMA DE TELEVISÃO PAGA, MÉTODO PARA REVOGAR DIREITOS EM TAL SISTEMA E MENSAGEM TRANSMITIDA PARA DECODIFICADOR

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

**(30) Prioridade Unionista:** 04/02/2003 FR 0301243

**(73) Titular(es):** NAGRA FRANCE SAS

**(72) Inventor(es):** JEAN-LUC DAUVOIS

Relatório Descritivo da Patente de Invenção para: **"SISTEMA DE TELEVISÃO PAGA, MÉTODO PARA REVOGAR DIREITOS EM TAL SISTEMA E MENSAGEM TRANSMITIDA PARA DECODIFICADOR".**

Descrição

Campo da Invenção

A presente invenção se refere a um sistema de televisão paga, um método para revogar direitos em tal sistema, decodificador e cartão inteligente associados e uma mensagem transmitida para tal decodificador. Em tais sistemas de televisão paga, dois modos bem conhecidos de distribuir programas audiovisuais podem existir quer separadamente ou em conjunto.

Um primeiro modo requer assinatura e/ ou pagamento como um pré-requisito para acesso descriptografado a programas audiovisuais. Nesse caso, o assinante tem que assinar e pagar periodicamente, por exemplo, todo mês, uma taxa de assinatura para acessar a transmissão de programas audiovisuais em um ou mais canais.

Um segundo modo apela para a oferta de visualização prévia temporária, não embaralhada, antes da assinatura ou pagamento. Nesse caso, o assinante é informado, por exemplo, por uma mensagem em sua tela que o acesso livre de cobrança e não codificado (ou seja, não embaralhado) a um

programa corrente ou prestes a começar foi concedido a ele para propósitos de pré-visualização ou o assinante solicita esse acesso. O assinante pode, assim, temporariamente visualizar um programa não codificado em um dado canal por um tempo de duração relativamente curto. Se o assinante deseja continuar a visualizar o programa, ele deve, antes de expirar esse tempo, realizar uma transação de pagamento por modem, por exemplo, de acordo com um esquema assim chamado *pay-per-view* ou esquema *pay-per-view* impulsivo, por exemplo, de acordo com mecanismos conhecidos por pessoas versadas na técnica. Se essa transação não for feita antes do fim do tempo, então, o acesso livre não codificado ao programa é interrompido e o programa, então, aparece embaralhado na tela da televisão do assinante.

A invenção é aplicável, em particular, aos dois modos acima mencionados, mas é mais particularmente descrita dentro da estrutura desse segundo modo.

No presente pedido de patente, os termos: programa audiovisual designa qualquer vídeo e /ou programa de áudio.

Estado da Técnica

As técnicas usadas em televisão paga são baseadas em dois mecanismos independentes: por um lado, em um embaralhamento / criptografação do programa de áudio e /ou vídeo (ou programas), ou por outro lado, em uma função para

alocação de direitos comerciais que são transmitidos como mensagens seguras para uma caixa de desembaralhamento ou para o decodificador (com acesso de controle). O embaralhamento/ criptografação pode ser aplicado facilmente a uma corrente de bits digital. Todos os bits podem ser embaralhados / criptografados usando, por exemplo, um cifrador de bloco inteligente. O embaralhamento é usado para transmissões analógicas. Por meio do uso de tal embaralhamento, o formato do sinal é alterado, os sinais de sincronização são suprimidos e enviados, em separado, na forma criptografada. O sinal de áudio pode ser convertido em sinal digital, então, criptografado. O sinal de áudio digital criptografado pode ser inserido no sinal de vídeo.

O programa audiovisual transmitido é embaralhado ou criptografado, usando chaves, que embaralham ou criptografam o programa audiovisual, pode ser desembaralhado ou descriptografado apenas através do uso de equivalentes dessas chaves, chamadas palavras de controle (CW). Em modo criptográfico simétrico, as chaves de criptografação / embaralhamento são iguais às palavras de controle. Em modo de criptografação assimétrico, as chaves de criptografação / embaralhamento são diferentes das palavras de controle. Para cada dado programa audiovisual, os valores da palavra de controle transmitidos para o

decodificador mudam periodicamente a uma freqüência relativamente alta, por exemplo, da ordem de um segundo. A fim de permitir a descriptografação na recepção do programa audiovisual, as mensagens de controle de alocação de direito ECM ("Mensagens de Controle de Direito") e mensagens de gerenciamento de alocação de direitos EMM ("Mensagens de Gerenciamento de Direito") são transmitidas para os decodificadores.

Esses dois tipos de mensagens ECM e EMM podem ser expedidos através do decodificador para um cartão inteligente ou qualquer objeto portátil, tal como cartão PCMCIA, uma chave inteligente..., que, em particular, forneça funções de descriptografação e armazenamento de direitos de usuário. Na presente descrição, o termo cartão designa qualquer objeto portátil operando em conjunto com o decodificador.

As mensagens ECM contêm palavras de controle criptografadas, as palavras de controle que permitem o decodificador desembaralhar / descriptografar um programa audiovisual. As mensagens ECM são transmitidas para o cartão que descriptografa as palavras de controle criptografadas e expede essas palavras de controle CW para o decodificador. O cartão realiza a operação de descriptografação das palavras de controle apenas se o

usuário estiver autorizado a acessar o programa de televisão corrente. Para esse propósito, o cartão armazena, em uma área da memória do mesmo, os direitos alocados ao usuário em questão. Assim, quando um usuário está associado por meio de assinatura com um cartão inteligente, a autorização de acesso é indicada por meio de dados de alocação de direitos ("dados de direito") armazenados no cartão.

As mensagens EMM contêm sinais que fazem com que seja possível atualizar os dados de alocação de direito do usuário, por exemplo, através da modificação de dados armazenados no cartão. No caso de uma oferta temporária de pré-visualização desembaralhada e de acordo com a técnica anterior, uma primeira mensagem EMM é expedida para o decodificador para oferecer temporariamente ao assinante os direitos requeridos para acessar um programa em dado canal. Ao insucesso de qualquer transação de pagamento recebida pelo sistema de gerenciamento de direitos do operador, uma outra mensagem EMM é expedida de forma a revogar esses mesmos direitos.

As mensagens ECM e EMM possuem um campo de assinatura digital que assegura a integridade da mensagem (por exemplo, um código hash). Isso torna possível detectar

qualquer corrupção malevolente ou acidental dos conteúdos da mensagem.

Uma mensagem ECM é emitida com o sinal embaralhado transmitido. Ela compreende três campos. O primeiro campo contém certos parâmetros de acesso. Esses parâmetros definem as condições sob as quais o acesso a um programa de televisão é permitido. Esse campo permite, por exemplo, apreciação de pais (um código PIN adicional é, então, requerido pelo decodificador) e restrição de difusão geográfica (um filme pode não ser disponibilizado em todos os países da Europa). Um segundo campo contém uma palavra de controle na forma criptografada. O último campo contém indicadores de controle de integridade de dados para a mensagem ECM em questão.

Uma mensagem EMM, tipicamente, compreende quatro campos. Cada mensagem EMM começa com um campo de endereço para seleção de um decodificador individual. Existem dois modos de endereçamento, um para um decodificador individual e o outro para um grupo de decodificadores. O segundo campo contém uma alocação de direitos para um dado usuário. O terceiro campo contém uma chave de operação na forma criptografada. O último campo contém indicadores de controle de integridade de dados para a mensagem EMM em questão. As mensagens EMM também podem ser usadas para

despachar um comando para o decodificador. A emissão de mensagens EMM é, em geral, o resultado de uma ação (assinatura) ou de um padrão de ação (não pagamento em modo "pague com pré-visualização temporária desembaralhada") do usuário para o operador. Essas mensagens são, em geral, individuais. O conteúdo das mesmas é interpretado por um decodificador (ou o cartão associado) ou por meio de um número limitado de decodificadores para os quais esses direitos particulares são relevantes. As mensagens EMM não são emitidas de forma síncrona com o programa de televisão ao qual elas se aplicam. Elas são transmitidas, antecipadamente, de forma a permitir a um usuário autorizado acessar um dado programa. Qualquer rede pode ser usada para transmitir essas mensagens EMM para o receptor: modem, mail, ou radio difusão.

Para estar certo que uma mensagem EMM foi recebida pelo usuário para uma assinatura, por exemplo, a última é expedida algumas vezes. As mensagens EMM são, assim, organizadas ciclicamente de acordo com um dado período para a emissão. A duração de tal período define o tempo de espera máximo a fim de obter uma alocação de direito para um usuário que desligou seu decodificador por uma grande duração.

Desse modo, estão representados, na figura 1, um embaralhador 10, desembaralhador 11 tipicamente integrado com um decodificador (não representado), um cartão inteligente 13 e mensagens ECM e EMM. O cartão inteligente 12 armazena em particular:

- um endereço de cartão, que é fixo;

- pelo menos uma chave de operação sk, que é atualizada periodicamente pela EMM;

- uma chave única Q, que é fixa.

Como anteriormente mencionado, uma mensagem ECM contém três campos contendo respectivamente:

- os parâmetros de acesso;

- uma palavra de controle criptografada por uma chave de operação, denotada por $E_{SK}CW$.

- um campo de controle de integridade de dados (código hash) para a mensagem ECM considerada.

Uma mensagem EMM contém quatro campos contendo respectivamente:

- um endereço;

- os direitos do usuário;

- uma chave de operação criptografada, denotada por $Sk:E_Q(sk)$;

- uma palavra de controle de integridade de dados (código hash) para a mensagem EMM considerada.

As palavras de controle CW sucessivas são expedidas para o embaralhador 10 e, em paralelo com o decodificador, de forma a permitir, respectivamente, o embaralhamento e / ou a criptografação e desembaralhamento e / ou descriptografação dos dados transmitidos.

Assim, os sinais de áudio e / ou vídeo podem ser embaralhados, usando-se palavras de controle (CW) sucessivas. Periodicamente, (por exemplo, a cada dez segundos) uma mensagem ECM é emitida com o sinal embaralhado. Essas mensagens ECM contêm as palavras de controle criptografadas pela chave de operação correntemente válida sk e transmitidas pela mensagem EMM de forma a armazenar no decodificador ou no cartão (por exemplo, cartão inteligente ou cartão PCMCIA), que está associado ao decodificador fornecido junto com a leitora de cartão.

As chaves de operação sk são atualizadas menos freqüentemente por mensagens EMM, por exemplo, todo mês. As chaves de operação sk são criptografadas com uma ou mais chaves Q únicas e individuais que são armazenadas de forma segura no cartão inteligente ou no decodificador.

Um problema de segurança pode aparecer nos sistemas de televisão paga que operam de acordo com um dos dois modos apresentados no início da descrição. Especificamente, a

revogação de direitos de assinatura de um programa, ou a revogação de direitos de assinantes é feita de acordo com a técnica anterior através da emissão de uma mensagem de assinante EMM (de tipo de mensagem EMM única ou EMM individual). Um pirata (ou "hacker") pode desejar de beneficiar de tal maneira de operação de forma a impedir tal revogação de ser efetivada após uma assinatura ter sido retirada ou uma pré-visualização desembaralhada temporária ter sido oferecida para o assinante por meio da expedição de uma mensagem de alocação de direitos EMM. O pirata pode, portanto, desenvolver uma técnica com a intenção de distinguir as mensagens ECM a partir das mensagens EMM. Ele pode, então, identificar e suprimir, através de filtragem, mensagens EMM, usando "bloqueadores". Tal técnica consiste, por exemplo, na tecnologia digital MPEG (*Moving Picture Expert Group*) na modificação de parâmetros de filtragem dos filtros MPEG de forma a não receber mensagens EMM até que uma mensagem EMM tenha sido recebida por um decodificador e até que os direitos do usuário tenham sido recebidos pelo decodificador (ou o cartão associado ao mesmo) através de uma mensagem EMM. O pirata pode, desse modo, por exemplo, filtrar e rejeitar todas as mensagens EMM, uma vez que um cartão tenha sido autorizado a desembaralhar um dado programa feito acessível em um modo de pré-visualização

desembaralhada temporário por meio de expedição posterior de mensagens EMM apropriadas. A supressão de mensagens EMM subseqüentes, após o acesso a um ou mais programas ter sido autorizado, previne modificações do estado de autorização.

Os dados de autorização, assim, não podem ser modificados e o acesso não autorizado a todos os programas transmitidos em um canal de pré-visualização desembaralhada e temporária é, assim, obtido por uma duração igual à duração da validade das chaves de operação armazenadas no cartão antes da filtragem das mensagens EMM.

A fim de resolver esse problema, a patente norte-americana US 5461675, que descreve um método de controle de acesso faz a previsão de um período de tempo durante o qual o cartão inteligente deve receber pelo menos uma mensagem EMM, dedicada ou de outra maneira ao cartão. Se esse requisito não for satisfeito, o cartão inteligente não fornece a informação correta para desembaralhar o programa audiovisual.

O objetivo da invenção é resolver o problema acima mencionado com uma solução diferente daquela descrita na patente norte-americana US 5461675, enquanto limita a largura de banda requerida para expedição de mensagens.

Descrição da Invenção

A presente invenção, portanto, propõe um método de revogar direitos de acesso a um programa audiovisual recebido por um decodificador compreendendo as etapas de:

- emissão de dois tipos de mensagens para o decodificador, as primeiras mensagens contendo palavras de controle criptografadas, cada palavra de controle sendo usada para desembaralhar durante um dado período de tempo o sinal audiovisual recebido, as segundas mensagens, cada uma, compreendendo indicações de alocação de direitos de usuário;

- descriptografação no decodificador ou em um objeto portátil associado com o mesmo das primeiras mensagens de forma a produzir palavras de controle para o desembaralhamento do referido sinal audiovisual recebido pelo decodificador, se o usuário estiver autorizado a acessar as indicações contidas nas mesmas,

caracterizado pelo fato de a emissão de terceiras mensagens híbridas, cada uma, resultando de uma combinação de pelo menos uma palavra de controle de um endereço de decodificador e de uma indicação de revogação de direitos.

O uso de mensagens híbridas (E3M) a fim de invalidar os direitos de assinatura ou os direitos do assinante torna possível garantir que a revogação será recebida (uma vez que sem a mensagem híbrida recebida, não existe possível

visualização de televisão) e, portanto, dispensa o tipo de pirataria de sistema acima aludida.

O método da invenção também faz com que seja possível reduzir a quantidade de mensagens expedidas. Não é mais, de fato, necessário expedir mensagens de gerenciamento alocação de direitos (EMM) a fim de suprimir uma oferta para um assinante. É possível fazer isso diretamente através do uso de uma mensagem híbrida E3M. Além das ofertas de assinaturas por si, é possível apagar assinaturas (chaves, dados de obsolescência, grupo) para um término de assinatura. Vantajosamente, em uma mensagem híbrida, a palavra de controle é criptografada por meio de uma chave de operação diferente da chave única a fim de criptografar o endereço do decodificador e a indicação de revogação de direitos. Vantajosamente, uma criptografia assimétrica pode ser usada.

A invenção também se refere a um sistema de televisão pago compreendendo uma unidade de gerenciamento de assinantes que armazena, na forma de um banco de dados, os identificadores de assinantes e seus direitos, uma unidade para criptografar mensagens EMM, um sistema que autoriza assinantes controlado pela unidade de gerenciamento de assinantes, um compressor MPEG de programas audiovisuais, uma unidade de cifragem de mensagens ECM, um embaralhador /

multiplexador, pelo menos um decodificador associado com um cartão inteligente, um servidor de comunicação, um supervisor conectado ao embaralhador / multiplexador e um link via satélite, terrestre ou por cabo entre o embaralhador / multiplexador e o decodificador, caracterizado pelo fato de compreender uma unidade para combinar campos de mensagem EMM e campos de mensagem ECM que compreendem, para cada canal de programa audiovisual individual pago, uma fila de mensagens EMM de revogação e um multiplexador, essa unidade para combinação dos campos sendo disposta na entrada do embaralhador / multiplexador.

A invenção também se refere a um cartão inteligente ou um decodificador para processamento de mensagens híbridas, que compreende meios para apagar os direitos registrados na memória do mesmo e descriptografar as palavras de controle criptografadas com a chave de operação corrente de forma a produzir palavras de controle.

A invenção, finalmente, refere-se a uma mensagem transmitida a pelo menos um decodificador em um sistema de televisão paga compreendendo pelo menos:

- um campo de palavra de controle criptografado, uma palavra de controle sendo pretendida para desembaralhar um sinal audiovisual recebido por um decodificador durante um dado período de tempo;

- um campo de endereço do decodificador; e

- um campo de revogação para direitos alocados para um (ou mais) decodificadores endereçados por um endereço no referido campo de endereço.

Breve Descrição dos Desenhos

A figura 1 ilustra um sistema de codificação / decodificação da técnica anterior que opera no campo da televisão digital.

A figura 2 mostra um diagrama de uma arquitetura geral de um sistema de televisão paga.

A figura 3 é um diagrama de blocos de uma unidade de combinação de campo de acordo com a invenção incluída em um multiplexador da arquitetura da figura 2.

Descrição Detalhada das Concretizações Particulares

No método da invenção, a supressão de direitos de acesso a pelo menos um canal que transite programas de pré-visualização desembaralhada e temporária é realizada com a ajuda de mensagens de um terceiro tipo, denotada E3M, diferentes das mensagens ECM e EMM.

Essas mensagens E3M transmitidas para pelo menos um decodificador no sistema de televisão paga compreendem pelo menos:

- um campo de palavra de controle criptografado;

- um campo de endereço de decodificador; e

- um campo de revogação para direitos alocados a um (ou mais) decodificador(es) endereçados por um endereço único ou agrupado no campo de endereço.

Cada mensagem híbrida compreende, além disso, tipicamente um campo de cabeçalho de identificador ECM diferente de um campo de cabeçalho de identificador EMM. Tais campos de cabeçalho de identificador tornam possível distinguir as mensagens ECM e EMM na recepção.

O fato de revogar direitos de acesso para um canal que transmite programas de pré-visualização desembaralhados e temporários em mensagens E3M, cada um incluindo uma palavra de controle e uma indicação de revogação de direitos limita a pirataria, uma vez que o pirata não pode usar um "bloqueador" por temer não ter mais acesso instantâneo, de alguma maneira, ao programa corrente, uma vez que ele, assim, bloqueia qualquer acesso a palavras de controle usadas para desembaralhamento do programa audiovisual desembaralhado.

Especificamente, um assinante acessando, a pedido ou através de uma oferta, um programa com pré-visualização temporária e desembaralhada (ou programa) em um dado instante e tendo cancelado o mesmo, mediante solicitação explícita ou através de padrão de transação, em um instante $t_0+\Delta t$ ($\Delta t$ possivelmente sendo um tempo bastante

curto) de modo a não pagar por essa oferta, poderia, previamente, usar um "bloqueador de EMM" nas mensagens EMM subseqüentes a fim de visualizar a oferta solicitada de graça (por uma escala de tempo máxima de dois ciclos de renovação, uma vez que, tipicamente cartões portáteis armazenam duas chaves de operação: a chave corrente e a chave futura).

Não é mais possível usar um "bloqueador de mensagens E3M", uma vez que bloquear as mensagens E3M eleva-se a barrar alguém de visualizar os programas solicitados.

A retirada de ofertas comerciais (ou o término da assinatura) é obtida por meio de mensagens E3M. cada mensagem E3M resulta da combinação de certos indicadores transmitidos por meio das mensagens ECM e de certos indicadores transmitidos pelas mensagens EMM, isto é, cada mensagem E3M compreende pelo menos uma palavra de controle criptografada, um endereço de decodificador e um indicador de revogação de diretos.

Conforme representado na figura 2, uma arquitetura dada por meio de exemplo de um sistema de televisão paga compreende uma unidade de gerenciamento de assinante (SMS) 20 que armazena, na forma de um banco de dados, os identificadores dos assinantes e seus direitos, e uma unidade de criptografação de mensagens EMM 21, um sistema

de autorização de assinantes 22 controlado pela unidade SMS, um compressor MPEG de programas audiovisuais 23, uma unidade de criptografação de mensagem ECM 24, um embaralhador / multiplexador 25, decodificadores 26 associados com respectivos cartões inteligentes 27, um servidor de comunicação 30 ligado ao sistema de autorização de assinantes 22 e aos decodificadores 26, um supervisor ligado ao embaralhador / multiplexador 25, e um link 32 via satélite, terrestre, ou por cabo entre o embaralhador / multiplexador 25 e o decodificador 26. Uma descrição detalhada da maneira de operação desse tipo de sistema é dada por exemplo no pedido de patente internacional WO98/43430.

Conforme representado na figura 3, a unidade para combinação de campos de mensagem EMM e campos de mensagem ECM compreende, tipicamente, para cada canal de programa audiovisual pago, uma fila de revogação EMM 40, bem como um multiplexador 41. Essa unidade para combinar campos é tipicamente disposta na entrada do embaralhador / multiplexador 25 da figura 2.

A sincronização das mensagens de mensagens ECM com o programa embaralhado é critica e as mensagens ECM não podem, portanto, ser retardadas nas filas.

Tipicamente, para um dado canal, assim que uma mensagem de revogação EMM é produzida, ela é armazenada na fila 40. Assim uma mensagem EMM é produzida (tipicamente a uma freqüência da ordem de um segundo), uma multiplexação é realizada de forma a combinar certas mensagens de revogação EMM e campos de mensagem ECM de forma a produzir uma mensagem E3M híbrida. Tal mensagem E3M, na saída do multiplexador 41, tipicamente compreende:

- um campo de palavra de controle criptografado, que se origina a partir de uma mensagem ECM;

- um campo endereço de decodificador que se origina de uma mensagem de revogação EMM; e

- um campo de revogação para direitos alocados ao decodificador ou ao conjunto de decodificadores endereçados por um endereço no referido campo de endereço, que se origina a partir da mesma mensagem EMM.

Especificamente, as mensagens EMM podem ser mensagens únicas, individuais ou de grupos.

Dado o ciclo de mudanças das mensagens ECM de entre 2 e 10 segundos, é possível ter um ciclo por hora de 300 a 1800 diferentes modificações.

A fim de tornar a pirataria impossível da parte de um usuário concorrente que pode conhecer as chaves de operação (pirataria que poderia consistir em expedir corretamente

mensagens de apagamento assinadas), esse apagamento pode ser feito através de uma mensagem EMM assinada por uma chave única Q do assinante, incluída na mensagem ECM (assinada e autenticada), usando-se uma chave de operação.

A principal restrição do método da invenção corresponde ao tamanho global de cada mensagem ECM, e também a duração do processamento do conteúdo dessas mensagens ECM.

Entretanto, tal restrição não é um inconveniente nos dias de hoje. O tamanho das mensagens ECM pode, de fato, atingir 256 bytes (sem usar o modo encadeado) e as memórias RAM dinâmicas existentes nos cartões inteligentes são amplamente suficientes.

Ademais, a velocidade dos processadores (CPU) e o uso de criptoprocessadores fazem com que seja possível obter um tempo de processamento adequado.

A fim de proibir qualquer ataque ao sistema originado de um usuário concorrente, uma criptografia do tipo assimétrica é usada. Especificamente, esse usuário não pode, então, gerar mensagens EMM ou ECM adaptadas por meio de cartões inteligentes dos assinantes se ele não tiver quebrado previamente as chaves assimétricas. Curvas elípticas ou algoritmos do tipo RSA podem ser assim usados. Algoritmos do tipo anterior têm a vantagem de requerer

menos espaço em memória e tornam possível ter conteúdos úteis de mensagens que são mais significantes.

Deve ser notado que, de acordo com a invenção, o cartão inteligente é capaz de processar três tipos de mensagem, isto é na maneira convencional:

- processar as mensagens EMM de forma a levar em conta as modificações dos direitos do assinante e da chave de operação que ela armazena na memória protegida do mesmo;

- descriptografação das palavras de controle criptografadas das mensagens ECM com a chave de operação corrente de forma a produzir palavras de controle; e

de acordo com a invenção:

- processar as mensagens híbridas E3M de forma a revogar direitos previamente alocados por meio de apagamento de direitos registrados na memória do mesmo, e descriptografação das palavras de controle criptografadas das mensagens E3M com a chave de operação corrente de forma a produzir palavras de controle.

Tal função pode também ser incluída no todo ou em parte em um decodificador ao invés de em um cartão.

**REIVINDICAÇÕES**

1. Método de revogação de direitos de acesso a um programa audiovisual recebido por um decodificador (11) compreendendo as etapas de:

- emissão de dois tipos de mensagens para o decodificador, as primeiras mensagens (ECM) contendo palavras de controle criptografadas, cada palavra de controle (CW) sendo usada para desembaralhar, durante um dado período de tempo, o sinal audiovisual recebido, as segundas mensagens (EMM), cada uma compreendendo indicações de alocação de direitos de usuário;

- descriptografação no decodificador ou em um objeto portátil associado com o mesmo das primeiras mensagens de forma a produzir palavras de controle (CW) para o desembaralhamento do referido sinal audiovisual recebido pelo decodificador (11), se o usuário estiver autorizado a acessar as indicações contidas nas mesmas;

**caracterizado pelo** fato de a emissão de terceiras mensagens híbridas (E3M), cada uma resultando de uma combinação de pelo menos uma palavra de controle, de um endereço de decodificador e de uma indicação de revogação de direitos.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de, em uma mensagem híbrida (E3M), a palavra de controle ser criptografada por meio de uma chave

de operação diferente a partir da chave única usada para criptografar o endereço de decodificador e a indicação de revogação de direitos.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de uma criptografia assimétrica ser usada.

4. Sistema de televisão paga compreendendo uma unidade de gerenciamento de assinante (20) que armazena os identificadores dos assinantes e seus direitos, uma unidade de criptografação de mensagens EMM (21), um sistema de autorização de assinantes (22), controlado pela unidade de gerenciamento de assinante (20), um compressor MPEG de programas audiovisuais (23), uma unidade de criptografação de mensagem ECM (24), um embaralhador / multiplexador (25), pelo menos um decodificador (26) associado com um cartão inteligente (27), um servidor de comunicação (30), um supervisor (31) e um link 32 entre o embaralhador / multiplexador (25) e os decodificadores (26), **caracterizado pelo** fato de compreender uma unidade para combinar campos de mensagem EMM e campos de mensagem ECM que compreende, para cada canal de programa audiovisual individual pago, uma fila de mensagens EMM de revogação (40) e um multiplexador (41), essa unidade para combinação dos campos sendo disposta na entrada do embaralhador / multiplexador (25).

5. Sistema, de acordo coma reivindicação 4, **caracterizado pelo** fato de compreender um cartão inteligente para processamento de mensagens híbridas transmitidas, tal como definidas em qualquer uma das reivindicações de 1 a 3, o cartão compreendendo meios para apagar os direitos registrados na memória do mesmo e descriptografar as palavras de controle criptografadas com a chave de operação corrente de forma a produzir palavras de controle.

6. Sistema, de acordo coma reivindicação 4, **caracterizado pelo** fato de compreender um decodificador para processamento de mensagens híbridas transmitidas, tal como definidas em qualquer uma das reivindicações de 1 a 3, o decodificador compreendendo meios para apagar os direitos registrados na memória do mesmo e descriptografar as palavras de controle criptografadas com a chave de operação corrente de forma a produzir palavras de controle.

7. Mensagem transmitida para pelo menos um decodificador em um sistema de televisão paga caracterizada por compreender pelo menos:

- um campo de palavra de controle criptografado, uma palavra de controle sendo pretendida para desembaralhar um sinal audiovisual recebido por um decodificador durante um dado período de tempo;

- um campo de endereço do decodificador; e

- um campo de revogação para direitos alocados para um (ou mais) decodificadores endereçados por um endereço no referido campo de endereço.

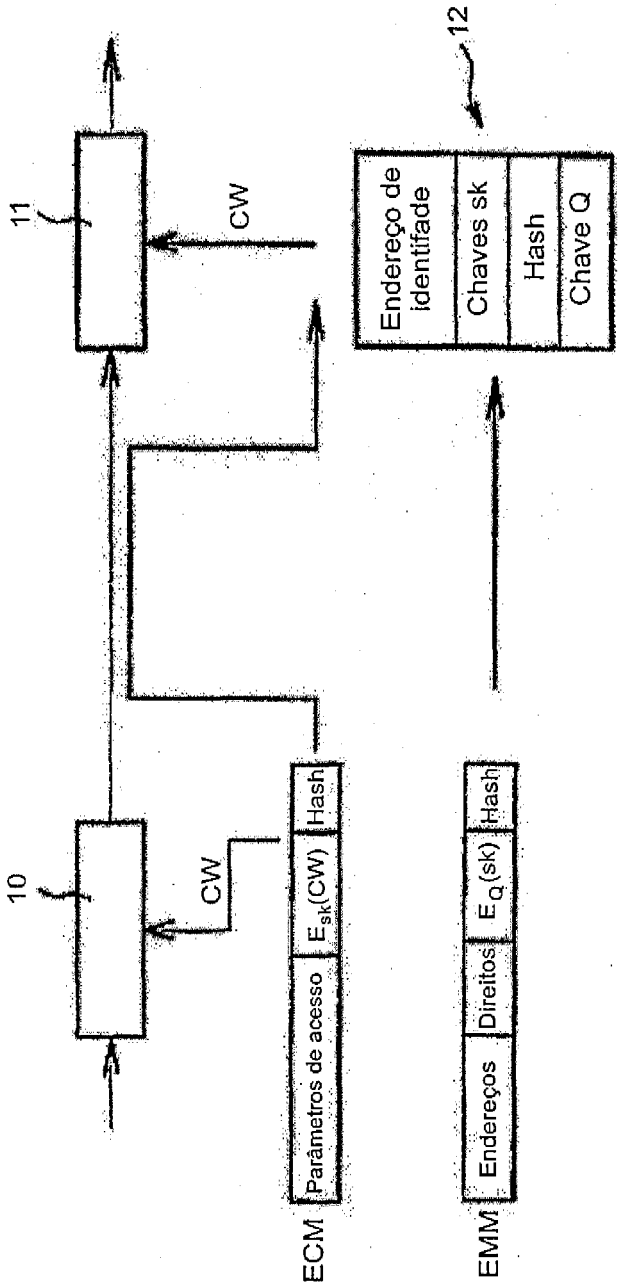
12
11
CW
Endereço de identifade
Chaves sk
Hash
Chave Q
10
CW
Hash
$E_{sk}$(CW)
Parâmetros de acesso
ECM
Endereços
Direitos
$E_Q$(sk)
Hash
EMM

FIGURA 1

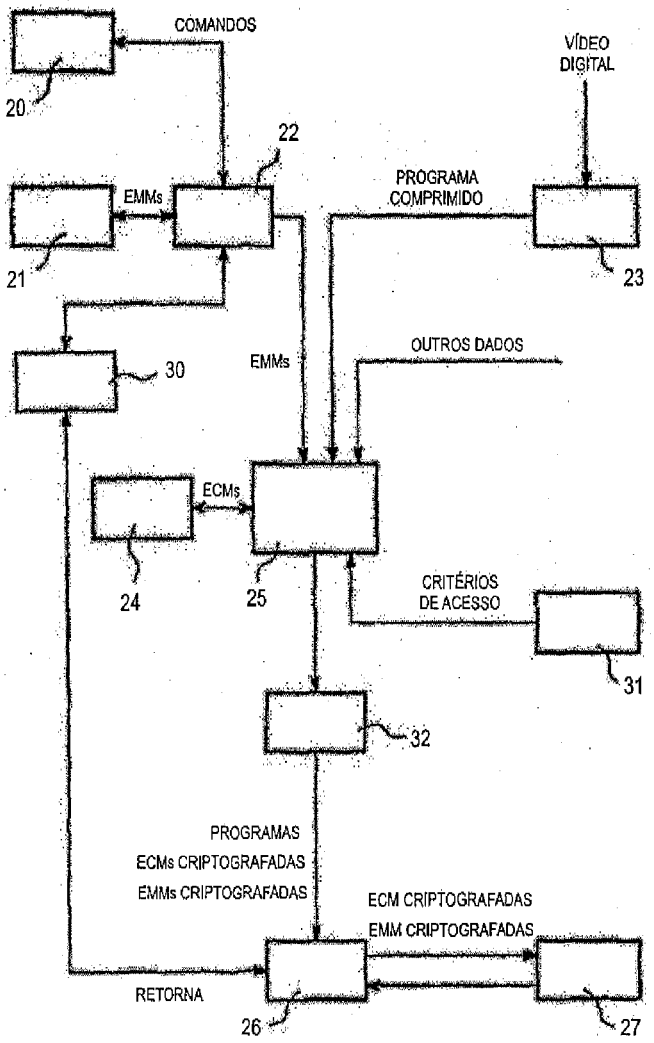
COMANDOS
20
22
VÍDEO
DIGITAL
EMMs
PROGRAMA
COMPRIMIDO
21
23
30
EMMs
OUTROS DADOS
ECMs
24
25
CRITÉRIOS
DE ACESSO
31
32
PROGRAMAS
ECMs CRIPTOGRAFADAS
EMMs CRIPTOGRAFADAS
ECM CRIPTOGRAFADAS
EMM CRIPTOGRAFADAS
RETORNA
26
27

FIGURA 2

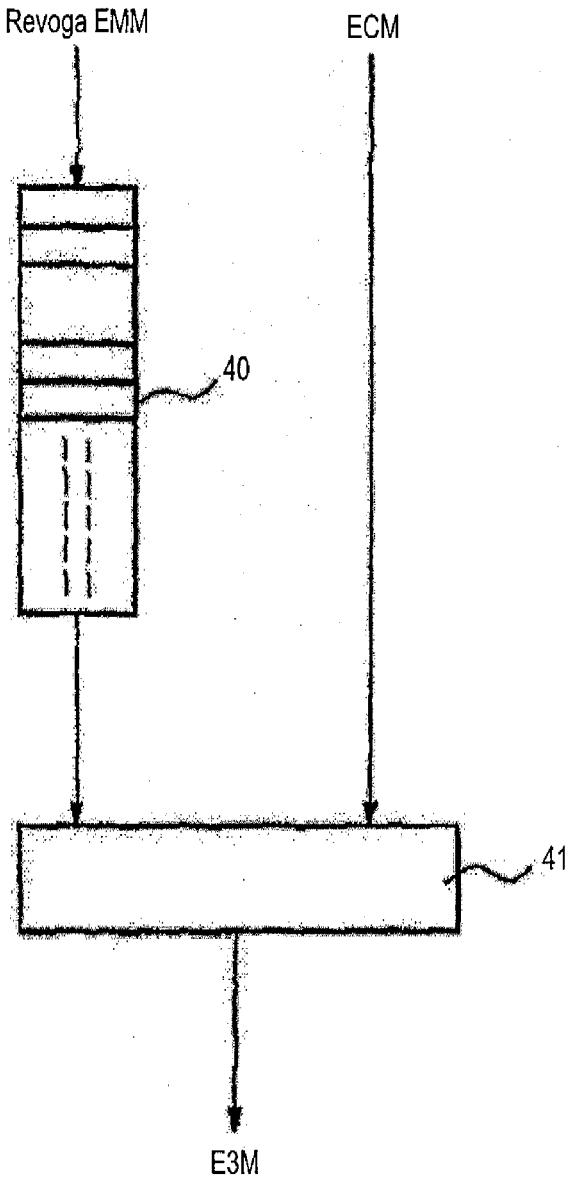


*FIGURA 3*