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

(11) PI 0309362-0 B1

(22) Data do Depósito: 15/04/2003

(45) Data de Concessão: 07/03/2017

(54) Título: MÉTODO PARA GERENCIAMENTO DOS DIREITOS DE UM CONTEÚDO CRIPTOGRAFADO EM UM GRAVADOR DIGITAL PESSOAL

(51) Int.Cl.: H04N 21/4408; H04N 21/426; H04N 21/4147

(52) CPC: H04N 21/4408,H04N 21/42623,H04N 21/4147,H04N 21/42661

(30) Prioridade Unionista: 19/04/2002 CH 0664/02

(73) Titular(es): NAGRAVISION SA

(72) Inventor(es): MARCO SASSELLI

Relatório Descritivo da Patente de Invenção para: **"MÉTODO PARA GERENCIAMENTO DOS DIREITOS DE UM CONTEÚDO CRIPTOGRAFADO EM UM GRAVADOR DIGITAL PESSOAL"**.

Campo da Invenção

O presente pedido se refere ao campo de receptores/ decodificadores de serviços de acesso condicional, particularmente de receptores que têm uma unidade de armazenamento, tal como discos rígidos.

Antecedentes da Invenção:

A evolução tecnológica no campo das capacidades de armazenamento e da velocidade dos discos magnéticos (discos rígidos) tem tornado possível armazenar o conteúdo de um vídeo transmitido para torná-lo acessível *off-line* para um usuário.

Esses gravadores são conhecidos pelos nomes comerciais ReplayTV ® ou Tivo ® e oferecem armazenamentos de diversas dezenas de horas de transmissão digital. Esses gravadores, porém, não são integrados, diretamente, nos receptores/ decodificadores de serviço de acesso condicional; particularmente, o conteúdo é armazenado sem proteção especifica no disco, o que torna impossível coletar os *royalties* do autores associados com o conteúdo no caso onde o disco será, então, duplicado com fins de redistribuição comercial.

Inversamente, em um sistema de televisão digital paga, o fluxo digital transmitido para esses receptores é criptografado a fim de ser capaz de controlar o uso e definir as condições para esse uso. Essa criptografação é realizada com palavras de controle que são mudadas em um intervalo regular (tipicamente, entre 5 e 30 segundos) de modo a dissuadir ataques tentando recuperar essa palavra de controle.

De acordo com uma concretização particular, as palavras de controle são mudadas em intervalos muito mais longos, o que significa que, para um dado evento, ele é criptografado por uma única palavra de controle.

Para o receptor ser capaz de descriptografar o fluxo criptografado por essas palavras de controle, estas últimas são enviadas para ele independentemente do fluxo nas mensagens de controle (ECM) criptografadas por uma chave específica para sistema de transmissão entre o sistema operacional (CAS) no módulo de segurança da unidade de usuário. De fato, as operações de segurança são realizadas em uma unidade de segurança (SC) que está, em geral, na forma de um cartão inteligente, dito ser inviolável. Essa unidade pode ser ou de um tipo removível ou pode ser integrada diretamente no receptor.

Durante a descriptografação de uma mensagem de controle (ECM), a presença do direito ao acesso ao fluxo considerado é verificada na unidade de segurança (SC). Esse direito pode ser administrado através de mensagens de autorização (EMM) que controlam esse direito na unidade de segurança (SC). Outras possibilidades são possíveis igualmente, tais como o envio de chaves de descriptografação.

Nesta descrição, usaremos o nome "evento" para um conteúdo de vídeo, áudio (por exemplo, MP3) ou dados (um programa de jogo, por exemplo) que é criptografado de acordo com método conhecido de palavras de controle, cada evento sendo capaz de ser criptografado por uma ou diversas palavras de controle, cada uma tendo uma duração determinada de validade.

A contagem de uso desses eventos é baseada hoje no princípio de assinatura, da compra de eventos ou do pagamento por unidade de tempo.

A assinatura permite definir um direito associado a um ou a diversos canais de transmissão desses eventos e permite ao usuário obter esses eventos na forma descriptografada se o direito estiver presente em sua unidade de segurança.

Ao mesmo tempo, é possível definir direitos que são específicos para um evento, tal como um filme ou uma partida de futebol. O usuário pode adquirir esse direito (através de compra, por exemplo) e esse evento será administrado especificamente com esse direito. Esse método é conhecido como *pay-per-view* (PPV).

Como para o pagamento por unidade de tempo, a unidade de segurança compreende um crédito que é debitado dependendo do consumo real do usuário. Dessa maneira, por exemplo, o crédito da unidade será debitado a cada minuto com base no canal ou evento selecionado. É possível, de acordo com as implementações técnicas, variar a unidade de contagem, ou na duração ou no valor do tempo atribuído, mesmo combinando esses dois parâmetros para adaptar o faturamento ao tipo de evento transmitido.

Uma mensagem de controle (ECM) contém não só a palavra de controle, mas também as condições para essa palavra de controle estar presente no receptor/ decodificador. Durante a descriptografação das palavras de controle, a presença na unidade de segurança de um direito ou habilitação, associada com as condições anunciadas de acesso na mensagem, será verificada.

A palavra de controle é retornada para a unidade de usuário apenas quando a comparação é positiva. Essa palavra

de controle está contida em uma mensagem de controle ECM, que é criptografada por uma chave de transmissão TK.

Para o direito estar presente na unidade de segurança, geralmente, ela é carregada nessa unidade por uma mensagem de gerenciamento de direito (EMM), que, por razões de segurança, em geral, é criptografada por uma chave diferente referida como uma chave de direito (RK).

De acordo com uma forma conhecida de transmissão de televisão paga, os três seguintes elementos são necessários para descriptografar um evento em um dado momento:

- o evento criptografado por uma ou diversas palavras de controle (CW);

- a mensagem ou mensagens de controle ECM contendo as palavras de controle (CW) e as condições de acesso (AC);

- o direito correspondente armazenado na unidade de segurança permitindo verificar as referidas condições de acesso.

De acordo com um projeto conhecido, o evento criptografado que é armazenado em uma unidade de armazenamento, tal como um disco rígido, é acompanhado por pelo menos uma ou diversas mensagens de controle ECM.

Devido ao fato de que a descriptografação *a posteriori* das mensagens de ECM pode ser um problema, particularmente por causa da mudança da chave transmissão, uma primeira

solução é proposta no documento EP 0 912 052, solução que implica na descriptografação dessas mensagens na unidade de segurança e re-criptografação antes do armazenamento no disco.

Essa solução resolve o problema da vida de trabalho da chave de transmissão, mas coloca uma grande carga de processamento na unidade de segurança no momento da gravação, sem saber se o conteúdo gravado um dia será usado. Além disso uma das regras fundamentais do sistema de segurança é retornar as palavras de controle para a unidade de usuário, apenas se os direitos existem. Nesse caso é muito provável que esses direitos não existam, se considerarmos um evento de *pay-per-view*. O direito será adquirido durante a compra, que pode ser feita muito mais tarde, quando o usuário decide ver esse evento.

Esse documento EP 0 912 052 não resolve o problema de acesso ao direito, visto que, no momento da compra, a mensagem de direito EMM tem que ser sempre transmitida de modo que ela seja carregada na unidade de segurança.

Dessa maneira, a solução descrita nesse documento é aplicável somente para eventos transmitidos para os quais o direito já está presente na unidade de segurança, a fim de autorizar a descriptografação e a re-criptografação da ECM.

Outro aspecto é conservação dos direitos de um portador. Tomemos, por exemplo, quando um portador A tem direitos de recepção dos canais M, N, P. Ele/ela tem, então, o direito de ver esses canais e, assim, gravar e ver à vontade os eventos que estão na sua unidade de armazenamento. Com cada uso desse evento, será requerido que a unidade de segurança descriptografe as mensagens ECM e retorne as palavras de controle. Então, é importante que os direitos ligados a esse evento estejam presentes na unidade de segurança.

No caso de um evento obtido por uma assinatura, a identificação desse evento está associada ao canal de assinatura, por exemplo, M. Assim todos os eventos que portem o identificador M estão autorizados e as palavras de controle são retornadas para o decodificador.

Esses direitos, então, são associados a um canal particular definido por um identificador, tal como M. Quando o assinante cancela sua assinatura ou modifica a mesma para outros canais, isso resulta em que os eventos gravados na unidade de armazenamento serão inacessíveis, porque a unidade de segurança recusará reenviar as palavras de controle, o direito correspondente não mais estando presente.

Essa situação também pode ocorrer se um novo identificador for atribuído ao canal M. Assim é possível que a re-organização dos canais atribua para esse canal o identificador J4, em lugar de M. Do ponto de vista dos direitos de transmissão, a unidade de segurança é informada sincronicamente da mudança e os registros do usuário não ficam em desacordo.

As conseqüências para um evento gravado são mais dramáticas. Essa reatribuição resultará no evento gravado se tornando inacessível, porque o direito correspondente não está mais presente na unidade de segurança.

Sumário da Invenção

O objetivo da presente invenção é proporcionar um método de armazenamento de um evento criptografado por palavras de controle (CW) que garante o acesso a esse evento em qualquer momento que seja desejado, mesmo se certas modificações ocorrerem entre o momento de armazenamento e o momento de visualização.

Esse objetivo é alcançado por um método de armazenamento de um evento criptografado por uma ou diversas palavras de controle (CW) em uma unidade de recepção e descriptografação (por exemplo uma *Set Top Box* ou STB) conectada a uma unidade de segurança (SC), essas palavras de controle (CW) e os direitos necessários estando

contidos nas mensagens de controle (ECM), caracterizado pelo fato de compreender as seguintes etapas:

- armazenamento do evento criptografado e das mensagens de controle (ECM) na unidade de armazenamento;

- transmissão das mensagens de controle (ECM) para a unidade de segurança (SC);

- verificação se os direitos de acesso a esse evento estão contidos na unidade de segurança (SC);

- determinação de um recebimento (Q) de toda ou parte da mensagem de controle (ECM), usando uma chave secreta (K) contida na unidade de segurança (SC) e específica para cada unidade de segurança;

- armazenamento desse recebimento (Q) na unidade de armazenamento.

De acordo com uma primeira concretização da invenção, esse recebimento é constituído por uma assinatura baseada em toda ou parte da mensagem de controle que constitui um super-direito que, então, permitirá o uso subseqüente do evento para verificar prioritariamente esse recebimento, antes da verificação dos direitos usuais na unidade de segurança. A presença desse recebimento, uma vez reconhecido por uma dada mensagem de controle, resulta nas condições de acesso usuais sendo ignoradas.

De acordo com uma segunda concretização da invenção, durante a geração do recebimento, à parte da assinatura, uma nova parte é adicionada que descreve como processar essa mensagem de controle quando ela é apresentada a essa unidade de segurança. Essa condição pode ser para ignorar todas as condições anunciadas nessa mensagem (que nos leva de volta à solução anterior) ou anunciar outras condições, tais como dispor de um direito de reprodução ou definir uma janela no tempo para autorizar essa reprodução.

Para determinar a assinatura, de preferência, tomaremos uma parte que não é mudada para todo o evento. De fato, a mensagem ECM compreende, esquematicamente, duas partes:

a) a palavra de controle para descriptografação (ou as palavras pares ou as palavras ímpares);

b) o direito necessário para retornar essa palavra de controle.

Esse recebimento permite a marcação de uma mensagem de controle e a adição de outra informação destinada ao processamento no modo de reprodução. O objetivo é, então, identificar uma mensagem de controle de maneira não ambígua. Na prática, que a parte b), quer dizer, o direito necessário, muda com menos freqüência que a palavra de controle. Isso é porque, de preferência, escolheremos essa

parte para calcular a assinatura. Não obstante, não é excluído determinar a assinatura na palavra de controle ou grupo das duas partes.

Para o cálculo dessa assinatura, determinamos uma única imagem da parte considerada através de uma função unidirecional e sem colisão com esses dados. É admitido que não existe um grupo diferente de dados que dê o mesmo resultado que essa função. Essa imagem H é produzida por uma função do tipo Hash (informação não válida). O algoritmo usado pode ser do tipo SHA-1 ou MD5 e essa imagem expressa o grupo de dados em uma única maneira.

A operação a seguir consiste na criptografação desses dados graças a uma chave de criptografação K.

Antes da operação de criptografação, pela chave K, é possível adicionar um campo de dados CD que descreve as novas condições de acesso. O grupo desse dados (H e CD) que constitui o recebimento é, então, criptografado com a chave de assinatura K.

No espírito da invenção o termo recebimento significa que é determinado por um grupo de dados que são representativos das condições de acesso (por exemplo, no caso mais simples) e únicos para uma unidade de segurança relacionada devido à chave de criptografação K. De acordo com uma concretização, é possível criptografar diretamente

as condições de acesso da mensagem de controle ECM por essa chave, sem passar através da operação de HASH.

De acordo com outra concretização, é possível determinar essa imagem única (função de HASH) nas condições de acesso e, então, criptografar essa imagem por meio de uma primeira chave K1, adicionar as novas condições de aceso CD e criptografar toda ela com a mesma chave K1 ou com uma segunda chave K2.

Breve Descrição dos Desenhos

A invenção será melhor compreendida com a ajuda da descrição detalhada a seguir, que faz referência aos desenhos anexos, que são dados como um exemplo não limitativo, a saber:

A figura 1 ilustra uma unidade de usuário STB com uma unidade de armazenamento, de acordo com uma concretização da invenção;

A figura 2 ilustra um grupo de dados armazenados na unidade de armazenamento da figura 1;

A figura 3 ilustra a estrutura de uma mensagem de controle ECM de acordo com uma concretização da invenção.

Descrição Detalhada da Invenção

O decodificador STB ilustrado na figura 1 recebe os dados de entrada na forma criptografada. Esses dados são armazenados na unidade de armazenamento HD e compreendem,

notavelmente, o evento considerado EV e as mensagens de controle ECM.

Dessa maneira, de acordo com a invenção, esses dois grupos de dados são acompanhados por um novo grupo que está ilustrado na figura 2 pelo bloco de recebimento Q.

O tamanho dos diferentes blocos é dado aqui como exemplo. Não obstante, podemos considerar que o evento EV ocupa a maior parte, as mensagens de controle ECM, uma pequena parte e, de acordo com uma concretização, um único recebimento é suficiente para o grupo desses dados.

De fato, se essa assinatura for realizada na parte das condições de acesso da mensagem de controle, ela não variará para todo o evento considerado.

Na figura 3 está ilustrada a estrutura de uma mensagem de controle ECM. Essa mensagem contém, como descrito previamente, a palavra de controle CW e as condições de acesso.

Essas condições são divididas em duas partes, uma parte específica para as condições de transmissão ACB e uma parte específica para as condições de reprodução ACR. Essa mensagem também compreende uma marca de tempo TP.

Entre essas condições podemos encontrar:

- o número do canal (ou serviços), particularmente útil para a assinatura;

- o tema do evento (por exemplo, esportes, notícias, adulto);

- o nível (tempo primário, tarde, retransmissão);

- um número para compra impulsiva.

A duplicação das condições abre possibilidades para o gerenciamento do evento durante a reprodução. O recebimento Q pode significar que é necessário se conformar simplesmente com as condições de reprodução ou pode significar, ao contrário, ignorar essas condições.

Vamos tomar como exemplo uma função de bloqueio geográfico. Essa função permite o bloqueio da recepção de eventos de esporte, por exemplo nas proximidades de 30 Km do estádio. Embora o bloqueio faça sentido no momento do evento, alguns dias mais tarde não há razão para esse bloqueio.

As condições de transmissão ACB podem inclui as transmissões do bloqueio por setor de números de unidade de segurança ou por código de endereçamento postal. As condições de reprodução ACR podem incluir uma simples autorização para tudo a partir de uma certa data (desde que as outras condições, tais como assinatura, sejam satisfeitas).

Durante a reprodução, o recebimento Q é acessado primeiro e descriptografado pela chave secreta K para obter a assinatura SGN e as novas condições de acesso CD.

A assinatura SGN, então, é retida na memória da unidade de segurança com as novas condições CD. Quando uma mensagem de controle ECM é apresentada a unidade de segurança, ela determina, pela função de HASH, uma imagem única H' na parte da ECM contendo os direitos AC e compara esse valor da imagem H' com a assinatura SGN de acordo com esse exemplo.

Se os dois valores forem idênticos, a unidade de segurança aplica as condições definidas na parte de condições CD do recebimento. Se essa condição CD for "acesso livre" isso elimina a exigência de verificar as condições contidas nas mensagem de controle ECM e, assim, elimina problemas causados pelas mudanças estruturais dos canais de transmissão.

De acordo com outra concretização, a nova condição CD reenvia as condições de reprodução ACR. Nessas condições não há referências aos canais ou outros elementos que poderiam variar em tempo (condições estruturais), mas condições no tempo durante o qual esse acesso é permitido ou um número de acessos de tempo permitidos. Deve ser compreendido, que, nesse caso, as condições de acesso

ligadas a uma assinatura ou outras foram verificadas durante a formação do recebimento.

O recebimento pode ser evolucionário. Em certos casos, pode ser de interesse armazenar um novo recebimento mais favorável do que o antigo. Esse é o caso, notavelmente, de uma compra impulsiva. Nesse caso, um primeiro recebimento é gerado durante o armazenamento, sem que o usuário tenha que comprar esse evento.

As condições contidas nesse recebimento reenviarão as condições contidas na mensagem de controle ECM.

No momento em que o usuário decide comprar esse evento, um novo recebimento é gerado, que abre a maneira para um uso sem reservas desse evento, se as condições são definidas como tal. Esse recebimento é, então, transmitido para a unidade de armazenamento para substituir o antigo.

REIVINDICAÇÕES

1. Método de armazenamento de um evento criptografado por uma ou diversas palavras de controle (CW) em uma unidade de recepção e descriptografia (STB) conectada a uma unidade de segurança (SC), as referidas palavras de controle (CW) e os direitos necessários para o acesso a esse evento estando contidos nas mensagens de controle (ECM), o método compreendendo as etapas a seguir:

armazenamento do evento criptografado, bem como da mensagem ou mensagens de controle (ECM) na unidade de armazenamento;

transmissão das mensagens de controle (ECM) para a unidade de segurança (SC);

verificação se os direitos de acesso a esse evento estão contidos na unidade de segurança (SC);

o método **caracterizado pelo** fato de que compreende as etapas de:

determinação de um recebimento (Q), que compreende uma assinatura (SGN) de toda ou parte da mensagem de controle (ECM) baseado em uma chave secreta (K) contida na unidade de segurança (SC) e específica para cada unidade de segurança;

armazenamento desse recebimento (Q) na unidade de armazenamento.

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de o recebimento (Q) ser calculado apenas se os direitos de acesso estiverem presentes na unidade de segurança.

3. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de o recebimento (Q) compreender também uma parte condicional (CD) descrevendo as novas condições independente da configuração estrutural da transmissão do evento.

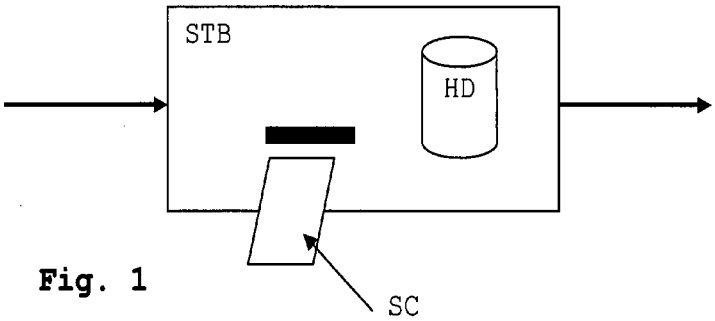

Fig. 1

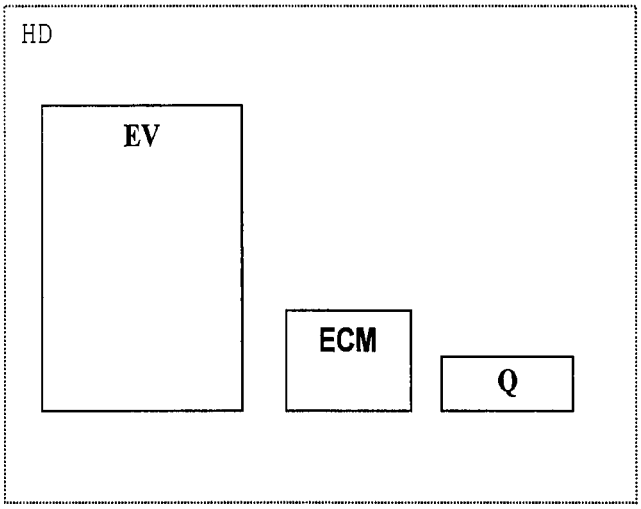

Fig. 2

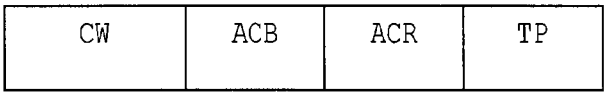

Fig. 3