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

(11) PI 1102971-4 B1

(22) Data do Depósito: 01/06/2011

(45) Data de Concessão: 14/12/2021

(54) Título: MÉTODO E APARELHO PARA DECRIPTOGRAFAR CONTEÚDO CRIPTOGRAFADO

(51) Int.Cl.: H04N 21/418; H04N 21/4623; H04N 21/442; H04N 21/6543; H04N 21/8358; (...).

(52) CPC: H04N 21/4181; H04N 21/4623; H04N 21/44236; H04N 21/6543; H04N 21/8358; (...).

(30) Prioridade Unionista: 01/06/2010 EP 10164592.0; 26/07/2010 US 61/367,473.

(73) Titular(es): NAGRAVISION SA.

(72) Inventor(es): MARCO MACCHETTI.

(57) Resumo: MÉTODO E APARELHO PARA DECRIPTOGRAFAR CONTEÚDO CRIPTOGRAFADO. A presente invenção fornece um método para decriptografar o conteúdo criptografado transmitido de um operador para uma pluralidade de usuários, onde a referida operadora fornece ainda a informação de segurança que permite a decodificação de tal conteúdo, O método tem a vantagem de satisfazer o objetivo de fornecer a capacidade para a detecção de um usuário fraudulento que retransmite as palavras de controle extraidas da informação de segurança para outros usuários. O método possibilita atingir esse objetivo, sem incorrer em sobrecarga adicional, além do conteúdo transmitido e informações de segurança. O método faz uso de palavras de controle que são baseadas em várias soluções fornecidas por colisões em funções matemáticas e envolve a observação das escolhas das palavras de controle retransmitidas pelo usuário fraudulento.

Relatório Descritivo da Patente de Invenção para: **"MÉTODO E APARELHO PARA DECRIPTOGRAFAR CONTEÚDO CRIPTOGRAFADO".**

Campo da Invenção

[0001] A presente invenção relaciona-se com o domínio dos sistemas de acesso condicional e, mais particularmente, a métodos para descobrir a identidade de um aparelho utilizado na prática da redistribuição não autorizada de chaves secretas de criptografia.

Descrição do Estado da Técnica

[0002] Uma área em que a presente invenção pode ser de interesse particular é no domínio da televisão por assinatura, em que o conteúdo de transmissão de áudio/vídeo proprietário é oferecido por um operador a uma taxa para uma pluralidade de consumidores assinantes. Sistemas de acesso condicional são empregados para lidar com o processamento de conteúdo de televisão por assinatura, com intuito de garantir que apenas os consumidores que assinaram determinados serviços, normalmente mediante o pagamento de uma taxa para o operador ou prestador desses serviços, na verdade, tiveram acesso ao conteúdo fornecido por esses serviços. De acordo com tais sistemas de acesso condicional, o conteúdo é codificado pelo operador sob as palavras de controle, o último sendo fornecido aos consumidores assinantes através de mensagens de segurança,

que são transmitidas em um fluxo de dados, juntamente com o conteúdo ou podem ser distribuídas através de outros meios. Cada consumidor assinante é fornecido com um receptor apropriado que compreende um módulo de segurança para permitir a extração das palavras de controle a partir das mensagens de segurança e uma unidade de desembaralhamento para decodificar o conteúdo de áudio/vídeo codificado difundido.

[0003] O conteúdo de áudio/vídeo criptografado tem valor e, como tal, os sistemas de acesso condicional têm sido alvo de ataque por terceiros mal-intencionados com a intenção de ter acesso ao conteúdo de áudio/vídeo sem assinar os serviços do operador e sem estar de posse dos equipamentos de recepção autorizados necessários. Uma prática conhecida como compartilhamento de palavra de controle, em que as palavras de controle transmitidas juntamente com o conteúdo criptografado são extraídas por um terceiro mal-intencionado usando módulos de segurança válidos e redistribuídas livremente para outros terceiros mal-intencionados, é uma ameaça particularmente significativa para os operadores que oferecem serviços de TV por assinatura, uma vez que os priva de receita de que teriam sido beneficiados.

[0004] Os operadores de televisão, portanto, têm um grande interesse em serem capazes de rastrear unidades receptoras que são usadas em atividades de compartilhamento de palavras de controle na medida em que isso permite que o operador tome medidas contra aqueles que estão envolvidos em tais atividades. O Pedido de Patente dos Estados Unidos No. 2002/0,133,701A descreve um método para a detecção de receptores traidores em um sistema de codificação de transmissão. O método inclui o uso de uma chave falsa para codificar subconjuntos plurais que representam os receptores do sistema. Os subconjuntos são derivados de uma árvore utilizando um sistema de Subconjunto-cobertura, e o receptor traidor é associado a uma ou mais chaves comprometidas que tenham sido obtidas por um receptor pirata potencialmente clonado. Utilizando um clone do receptor pirata, a identidade do receptor traidor é determinada. Este sistema, no entanto, tem a desvantagem de que várias codificações do mesmo conteúdo têm de ser transmitidas, tendo assim um impacto negativo na eficiência da largura de banda de transmissão.

Sumário da Invenção

[0005] Como descrito acima, a fim de combater as atividades de compartilhamento de palavras de controle, existe uma necessidade de proporcionar um método de

rastreio de traidor que seja simples de implementar e que não tenha um impacto negativo sobre a largura de banda de transmissão. Com este objetivo em mente, a presente invenção proporciona um método para decodificar o conteúdo de áudio/vídeo codificado em um decodificador, compreendendo pelo menos um desembaralhador e um módulo de segurança, a referida decodificação sendo realizada pelo decodificador utilizando uma palavra de controle final, o referido método compreendendo as seguintes etapas:

- receber, pelo módulo de segurança, pelo menos duas palavras de controle a partir de qualquer uma das quais a palavra de controle final é derivável;

- receber, pelo decodificador, o conteúdo de áudio/vídeo codificado;

- selecionar, pelo módulo de segurança, uma das pelo menos duas palavras de controle;

- transferir a palavra de controle selecionada para o desembaralhador;

- converter, pelo desembaralhador, a palavra de controle selecionada para a palavra de controle final, utilizando, pelo menos, uma primeira função criptográfica, a referida função criptográfica produzindo a mesma palavra de controle final durante pelo menos duas palavras de controle diferentes;

– usar a palavra controle final para decifrar o conteúdo de áudio/vídeo criptografado.

[0006] Ao criar uma relação entre uma sequência de palavras de controle selecionadas a partir de uma sequência de pares de palavras de controle por um lado, e um ponto de referência que identifica unicamente um módulo de segurança por outro lado, o método proporciona a capacidade de identificar um módulo de segurança utilizado em atividade de compartilhamento de palavra de controle. Pensando que as palavras de controle recebidas foram as palavras de controle finais, a intenção do usuário malicioso em realizar a atividade de compartilhamento de palavra de controle seria redistribuir as palavras de controle selecionadas ao invés das palavras de controle finais. O resultado, por um lado, é que outros usuários maliciosos que recebem as palavras de controle compartilhadas não seriam capazes de decodificar o conteúdo codificado, e, por outro lado, o usuário mal-intencionado, instigador da atividade de compartilhamento de palavra de controle, colocava-se aberto à descoberta de sua identidade pelo operador, que observa as palavras de controle redistribuídas. Assim, a invenção proporciona uma solução eficaz e facilmente realizável para o problema da detecção

de traidor onde um assim chamado traidor une-se a um sistema de compartilhamento de palavra de controle.

Breve Descrição das Figuras

[0007] A presente invenção será melhor compreendida graças à descrição detalhada a seguir e aos desenhos anexos, que são dados como exemplos não limitativos de concretizações da invenção, em que:

[0008] A Fig. 1 mostra um diagrama de blocos que ilustra um sistema de acesso condicional CAS, em que uma concretização da presente invenção pode ser implantada.

[0009] A Fig. 2 mostra um diagrama de blocos de um decodificador DEC, em que outra concretização da presente invenção pode ser implementada.

Descrição Detalhada da Invenção

[00010] O método utilizado na presente invenção faz uso do fenômeno de colisões em certos tipos de funções matemáticas e aproveita os diferentes níveis de complexidade associados com o encontro de tais colisões. Por exemplo, para um dado primeiro operando CW1, é possível encontrar uma função criptográfica H, a qual irá produzir um resultado CW. Além disso, é possível encontrar um segundo operando CW2, diferente do primeiro operando CW1, sobre o qual a aplicação da mesma função criptográfica H irá produzir o mesmo resultado CW. Em outras palavras, é

possível encontrar uma colisão, onde dois operandos diferentes CW1, CW2 submetidos a uma função criptográfica H produzem o mesmo resultado CW. No caso em que a função criptográfica H é uma função hash de 64 bits, seriam necessários cerca de 2^{32} operações para localizar uma tal colisão, o que é praticamente impossível usando a tecnologia atualmente disponível. No entanto, para encontrar uma colisão adicional, pela qual um terceiro operando CW3 produz o mesmo resultado CW quando submetido à função criptográfica H, exigiria cerca de 2^{64} operações, o que é tecnicamente impraticável usando a tecnologia atualmente disponível.

[00011] Em um sistema de acesso condicional padrão em que um operador deseja transmitir conteúdo de áudio/vídeo de maneira segura de uma cabeça de rede a uma pluralidade de decodificadores, ele criptografa o conteúdo sob as palavras de controle na cabeça de rede e transmite o conteúdo criptografado. Ele também criptografa as palavras de controle em uma chave de transporte e inclui os resultados em mensagens de segurança que também devem ser transmitidas a partir da cabeça de rede. Como é bem conhecido na indústria da televisão por assinatura, o conteúdo codificado AVE e as mensagens de segurança ECM são normalmente transmitidos em um fluxo de dados DS e

filtrados pelo decodificador para posterior processamento por vários módulos no decodificador. Os decodificadores que possuem módulos de segurança com acesso à chave de transporte ou uma tecla equivalente e, portanto, seriam capazes de extrair as palavras de controle recebidas nas mensagens de segurança de transmissão. Além disso, de acordo com princípios bem conhecidos na indústria de televisão por assinatura, antes de ser autorizada a decriptografar uma ECM, uma verificação é feita para verificar se o módulo de segurança realmente tem os direitos necessários para ser capaz de decodificar o conteúdo. Estes direitos são geralmente obtidos mediante o pagamento de uma taxa e os direitos são carregados no módulo de segurança por meio de outro tipo de mensagem de segurança conhecido como mensagens de gerenciamento de habilitação EMM, que podem ser recebidas quer no canal de transmissão, juntamente com o conteúdo, ou por outro canal. Este segundo tipo de mensagem de segurança é endereçável a um único ou a um grupo de módulos de segurança. Podemos ver então que a transmissão de conteúdo de acesso condicional é feita, portanto, em três partes: a criptografia de conteúdo sobre palavras de controle, a criptografia das palavras de controle para formar ECMs – que podem ser decriptografadas por módulos de segurança com os direitos necessários e, em

terceiro, a concessão de direitos e manuseio de tais direitos utilizando EMMs endereçáveis.

[00012] Por outro lado, de acordo com uma concretização do presente invenção, o fenômeno de colisão descrito acima é explorado num sistema de acesso condicional CAS na qual um operador OP transmite a partir de uma cabeça de rede HE para pelo menos um decodificador DEC. Neste caso, o conteúdo AV foi criptografado AVE com a cabeça de rede HE com pelo menos uma palavra de controle final CW ou uma chave KE, que é derivada a partir da palavra de controle final CW. Em vez de incluir a palavra de controle final CW nas mensagens de segurança ECM para serem transmitidas com o conteúdo criptografado AVE, as mensagens de segurança ECM, cada uma, compreendem pelo menos uma primeira e uma segunda palavras de controle CW1, CW2. Cada uma das palavras de controle CW1, CW2 na mensagem de segurança ECM representa uma colisão para uma dada função criptográfica H, em que a função criptográfica H de cada uma dentre a primeira ou segunda palavras de controle de CW1, CW2 produz a mesma palavra de controle final única CW. O decodificador DEC tem acesso a um módulo de segurança SM e um desembaralhador DESC como mostrado na Fig. 1. O decodificador DEC recebe o conteúdo codificado AVE e pelo menos uma mensagem de segurança ECM da cabeça de rede HE. O

módulo de segurança SM extrai e seleciona uma dentre a primeira ou segunda palavras de controle de CW1, CW2 e a transfere para o desembaralhador DESC para ser convertida para a palavra de controle final CW com a função criptográfica H. O desembaralhador DESC, então decriptografa o conteúdo criptografado AVE em um módulo de decodificação DECR usando a palavra controle final CW ou uma chave KE, que se deriva da palavra de controle final CW. Numa concretização particular da invenção, a função criptográfica H, que é usada é uma a função hash ou de 64 bits de sentido único.

[00013] Em um ataque de compartilhamento de palavra de controle, um usuário mal-intencionado de um módulo de segurança válido SM retransmite as palavras de controle finais CW que foram decodificadas com sucesso a partir das mensagens de segurança ECM recebidas pelo módulo de segurança válido SM, para qualquer número de usuários com equipamento de decodificação não autorizado (isto é, desembaralhadores sem módulos de segurança ou desembaralhadores com módulos inválidos de segurança), permitindo, assim, que os usuários não autorizados decriptografem o conteúdo criptografado a partir da cabeça de rede diretamente ao usar as palavras de controle finais CW fornecidas pelo usuário mal-intencionado. Um dos meios

disponíveis para a retransmissão é a internet e por isso é fácil ver porque essa atividade é uma séria ameaça para os operadores de conteúdos de difusão valiosos. O recurso de rastreabilidade proporcionado pela presente invenção resulta do modo em que o módulo de segurança é instruído para selecionar entre as duas palavras de controle CW1, CW2 e do fato de que o operador OP também escuta as palavras de controle CW sendo compartilhadas por um usuário mal-intencionado.

[00014] Em um sistema de acesso condicional padrão CAS, o equivalente da palavra de controle final CW descrita acima é transferido do módulo de segurança para o desembaralhador DESC. Em um sistema de acesso condicional CAS, no qual uma concretização da presente invenção é implantada, o usuário mal-intencionado vai confundir a palavra de controle CW1, CW2 a partir do módulo de segurança SM com a palavra de controle final CW e erroneamente distribuirá a palavra de controle CW1, CW2. Isso tem dois efeitos: por um lado impede que outros usuários mal-intencionados que recebam as palavras de controle acessem o conteúdo criptografado AVE, pois o conteúdo criptografado é criptografado sob as palavras de controle finais CW e, por outro lado, se a escolha de palavras de controle CW1, CW2 pode estar relacionada a um

parâmetro que pode identificar um módulo de segurança SM, em seguida, o usuário mal-intencionado coloca-se aberto à descoberta por um operador que observa uma série de palavras de controle compartilhadas CW1, CW2. Isto é explicado mais abaixo.

[00015] Cada módulo de segurança SM em uma coleção de módulos de segurança SM geridos pelo operador OP é unicamente identificado por uma definição interna UA, que é especial para o módulo de segurança SM. Cada módulo de segurança SM é instruído a selecionar uma das palavras de controle CW de acordo com sua configuração interna exclusiva UA. A configuração interna UA pode ser, por exemplo, o valor de um registro que representa o endereço único do módulo de segurança. De preferência, o módulo de segurança SM é instruído para selecionar a palavra de controle CW de acordo com o valor do bit de ordem n do seu endereço único, por exemplo.

[00016] Numa concretização em que as palavras de controle não estão agrupadas em pares, como mencionado acima, mas em grupos de palavra 16 ou 32 palavras de controle, um dos quais deve ser selecionado de acordo com uma configuração interna, então em vez de usar apenas um bit da configuração interna (UA) para a seleção, um bloco de bits pode ser usado para fazer a seleção. Por exemplo,

no caso de um único endereço de 32 bits que se pode dividir os 32 bits em 8 blocos de 4 bits e realizar uma operação matemática nos 4 bits e utilizar o resultado para indicar a seleção. Em seguida, passamos para o próximo bloco e fazemos o mesmo de novo e assim por diante.

[00017] De acordo com uma concretização da presente invenção, uma série de pares de primeira e segunda palavras de controle CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n são recebidos pelo módulo de segurança SM e, para cada par de palavras de controle CW1, CW2 na série CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n, o módulo de segurança SM é instruído para selecionar uma do par CW1, CW2 de acordo com o valor de um determinado bit em seu endereço original. Por exemplo, a seleção a partir do primeiro par de palavras de controle CW1a, CW2a é feita de acordo com o valor do primeiro bit de endereço do módulo de segurança SM único, enquanto a seleção a partir de um segundo par de palavras de controle CW1a, CW2a é feita de acordo com o valor do segundo bit de um endereço único e assim por diante. O resultado é que cada módulo de segurança SM irá selecionar um conjunto de palavras de controle a partir dos pares de palavras de controle CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n de acordo com o valor do seu endereço único, isto é, numa única maneira. Ao inspecionar a série de palavras de

controle utilizada por um módulo de segurança SM ou, mais exatamente, redistribuída por um usuário mal-intencionado de um módulo de segurança SM, é possível, portanto, para o operador OP, deduzir o endereço exclusivo do módulo de segurança, uma vez que o operador OP mantém o controle de todos os pares de palavras de controle enviadas CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n. Por espionagem OBS, a fim de pegar as palavras de controle que o usuário de um módulo de segurança SM pode transmitir a outros usuários, o operador OP pode detectar qual o desembaralhador DEC, ou pelo menos qual o módulo de segurança SM que está transmitindo as palavras de controle CW e tomar medidas adequadas contra o usuário do desembaralhador DEC. A presente invenção, portanto, proporciona um método simples para a detecção de um módulo de segurança SM, que é utilizado num sistema de compartilhamento de palavra de controle pela simples observação OBS das palavras de controle CW retransmitidas ao longo do tempo. O método quase não tem efeito negativo sobre a largura de banda de transmissão uma vez que não há sobrecarga de transmissão significativa necessária, acima das exigências normais de transmissão de radiodifusão. O método serve tanto para identificar o aparelho raiz do uso malicioso e para evitar que outros usuários tenham acesso ao conteúdo criptografado usando as palavras de controle

redistribuídas já que o conteúdo é criptografado usando palavras de controle finais CW e não usando as palavras de controle CW1, CW2.

[00018] Como foi anteriormente mencionado, pode demorar cerca de 2^{32} operações para localizar uma colisão no caso em que a função H é uma função hash de 64 bits. Em outras palavras, para uma dada primeira palavra de controle CW1, levando a uma dada palavra de controle final CW por meio da função H, que iria levar até 2^{32} operações para localizar uma segundo palavra de controle CW2, o que levaria à mesma palavra de controle final CW. Isso é tecnicamente viável usando a tecnologia disponível atualmente. No entanto, para encontrar uma colisão adicional, isto é, uma terceira palavra de controle CW3, que teria como resultado a mesma palavra de controle final CW, utilizando a mesma função H, levaria 2^{64} operações, o que se torna tecnicamente impraticável. Isto significa que é mais fácil para o operador OP encontrar um par de palavras de controle CW1, CW2, que vai dar a mesma palavra de controle final CW quando submetido à função H, mas tecnicamente impraticável para um terceiro malicioso descobrir uma terceira palavra de controle CW3, que daria a mesma palavra de controle final CW quando submetida à função H. Por sucessivamente retransmitir, como parte de um

esquema de compartilhamento de palavra de controle, uma das duas palavras de controle CW1, CW2 recebida em uma transmissão, a identidade de um terceiro mal-intencionado é passível de ser comprometida se o operador OP simplesmente observa OBS a série de palavras de controle CW1, CW2 sendo compartilhadas.

[00019] O mecanismo descrito acima para selecionar qual das duas palavras de controle de um par CW1, CW2, deve ser usada pelo módulo de segurança SM pode ser substituído ou ativado/desativado. Para substituir, por exemplo, a cabeça de rede iria enviar a mensagem de segurança ECM, que inclui as duas palavras de controle CW1, CW2 como antes e também incluem uma instrução para desativar a seleção com base na configuração interna. O ECM poderia incluir uma instrução a respeito de que a palavra de controle para selecionar, assim, substituindo o sistema de seleção pela configuração interna. Numa outra concretização, uma mensagem de segurança separada ou uma mensagem de gerenciamento EMM pode ser usada para dar instrução de ativar/desativar ou para dar a instrução que indica qual das duas palavras de controle recebidas numa mensagem de segurança anterior ou numa mensagem de segurança deve ser usada futuro. Em ainda outra concretização da presente invenção, as instruções podem vir de uma forma indireta.

Por exemplo, a mensagem de segurança ECM, ou uma mensagem de gerenciamento EMM pode ainda compreender informação de tempo, tais como hora do dia, por exemplo. A instrução de qual a palavra de controle a ser utilizar pode ser o resultado de alguns cálculos intermediários que utilizam a informação de tempo na mensagem de segurança ECM ou na mensagem de gerenciamento EMM, ou um seu derivado. Além disso, qualquer destas mensagens acima descritas poderia ser utilizada para fornecer instruções para indicar a um módulo de segurança que ele deve usar alguma outra configuração interna, tal como um valor de crédito, por exemplo, como critérios de seleção. É também possível para instruir o módulo de segurança para executar manipulações matemáticas em qualquer uma das configurações internas para derivar de um modo mais indireto do parâmetro de seleção.

[00020] Numa concretização particular da presente invenção, um contador de varredura inicializado CNTR é utilizado para apontar para um bit particular no endereço único dos módulos de segurança. Quando inicializado, o contador de varredura aponta para o primeiro bit do endereço único e o estado deste bit é utilizado para selecionar um dentre um primeiro par de palavras de controle recebidas. Quando a seleção foi feita, o contador de varredura incrementa e o próximo bit do endereço único é

usado para selecionar um a partir do próximo par de palavras de controle recebido. Este processo é contínuo até que todos os bits do endereço único sejam utilizados, após o qual o contador de varredura é reinicializado. As palavras de controle a partir das mensagens de segurança podem ser tratadas à medida que eles chegam, ou podem ser armazenadas numa tabela de palavra de controle CWT e processadas a pedido ou de acordo com um regime com base no tempo.

[00021] De acordo com outra concretização da presente invenção, em vez do processamento de comando orientado descrito acima, um método mais automatizado pode ser utilizado. Nesta concretização, a mensagem de segurança ECM ou a mensagem de gerenciamento EMM compreende ainda informações relacionadas com o tempo – a hora do dia, por exemplo. Esta informação pode ser usada para indicar ainda em que momento da seleção da palavra de controle deve ser feita. Além disso, uma função hash executada na informação relacionada com o tempo produz um valor que pode ser utilizado para apontar para um bit particular do endereço ímpar para utilizar na seleção de um a partir do par de palavras de controle. Por exemplo, para um endereço de 32 bits único, um modulo 32 do resultado do hash das

informações relacionadas com o tempo apontariam para um dos 32 bits do endereço único.

[00022] A Fig. 2 mostra um diagrama esquemático de uma outra concretização de um desembaralhador DEC, em que uma concretização da presente invenção pode ser implantada. Nesta concretização, uma camada adicional de criptografia é acrescentada. O objetivo aqui é oferecer outras possibilidades de aumentar a complexidade de um algoritmo de criptografia proprietária usada na implementação da invenção, ofuscando, assim, ainda mais a palavra de controle final se um usuário mal-intencionado tiver acesso à tabela de palavra de controle CWT. Nesta concretização, uma segunda função criptográfica F é primeiro aplicada à palavra de controle selecionada CW1, CW2, utilizando uma chave de criptografia intermediária KI. Vale a pena notar que a chave intermediária Kl usada na segunda função criptográfica F pode ser ligada no interior do desembaralhador DESC, sendo, de preferência, um desembaralhador proprietário. Esta segunda função criptográfica F produz uma palavra de controle intermediária CIO, que é, em seguida, dividida numa primeira parte CWI1 e numa segunda parte CWI2. A primeira parte CWI1 é, então, submetida à primeira função criptográfica H para dar uma palavra de controle parcial

CWP. A palavra de controle parcial é, então, concatenada CONC ou, de algum modo, combinada com a segunda parte CWI2 para dar a palavra de controle final CW. Deve ser notado que, durante a divisão da palavra de controle intermediária CIO, é dada atenção ao fato de que uma primeira parte CWI1 obtida a partir de qualquer uma das duas palavras de controle CW1, CW2 deve produzir a mesma palavra de controle parcial CWP quando submetida à primeira função criptográfica H. De igual modo, a palavra de controle final CW, resultante da combinação de palavra de controle parcial CWP e da segunda parte CWI2 será a mesma independentemente de qual das duas palavras de controle CW1, CW2 seja selecionada.

[00023] De acordo com uma concretização da invenção, a segunda função criptográfica F é, de preferência, uma função criptográfica simétrica tal como é geralmente conhecida no domínio criptográfico, como, por exemplo, o algoritmo de codificação de bloco padrão de criptografia de dados DES, ou o padrão de criptografia avançado (*Advanced Encryption Standard* AES), por exemplo.

REIVINDICAÇÕES

1. Método para decriptografar conteúdo de áudio/ vídeo criptografado (AVE), em um decodificador (DEC), compreendendo pelo menos um desembaralhador (DESC) e um módulo de segurança (SM), a referida decriptografia sendo realizada pelo desembaralhador (DESC), utilizando pelo menos uma palavra de controle final (CW), o referido método **caracterizado pelo** fato de que compreende as etapas de:

- receber, pelo módulo de segurança (SM), pelo menos duas palavras de controle (CW1, CW2) das quais uma primeira palavra de controle final (CW) é derivável;

- receber por meio do desembaralhador (DESC), o conteúdo de vídeo/ áudio criptografado (AVE);

- selecionar, pelo módulo de segurança (SM), uma das pelo menos duas palavras de controle (CW1, CW2), a referida seleção com base em pelo menos uma primeira parte (UA1) de uma configuração interna que permite que o módulo de segurança (SM) seja unicamente identificado (UA);

- transferir a palavra de controle selecionada (CW1, CW2) para o desembaralhador (DESC);

- converter, por meio do desembaralhador (DESC), a palavra de controle selecionada (CW1, CW2) para a primeira palavra de controle final (CW) usando pelo menos uma primeira função criptográfica (H), a referida função criptográfica (H) produzindo a mesma palavra de controle final (CW) para pelo menos duas palavras de controle diferentes (CW1, CW2);

- usar a primeira palavra de controle final (CW) para

decriptografar pelo menos uma primeira parte do conteúdo de áudio/ vídeo criptografado (AVE)

- receber, pelo módulo de segurança (SM), pelo menos um primeiro conjunto adicional de pelo menos duas palavras de controle (CW1a, CW2a) das quais uma palavra de controle final adicional é derivável;

- adicionalmente, selecionar pelo módulo de segurança, uma palavra adicional dentre as duas palavras de controle (CW1a, CW2a) a partir do conjunto adicional de duas palavras de controle (CW1a, CW2a), a referida seleção adicional baseada em pelo menos uma segunda parte (UA2) da configuração interna (UA), a referida segunda parte (UA2) da configuração interna (UA) sendo diferente da primeira parte (UA1) da configuração interna (UA);

- transferir a palavra de controle selecionada adicional (CW1a, CW2a) para o desembaralhador (DESC);

- converter, pelo desembaralhador (DESC), a palavra de controle adicional selecionada (CW1a, CW2a) para a palavra de controle final adicional (CW) usando pelo menos a primeira função criptográfica (H), a referida função criptográfica (H) produzindo a mesma palavra de controle final adicional para pelo menos duas palavras de controle diferentes (CW1a, CW2a);

- usar a palavra de controle final adicional (CW) para decriptografar pelo menos uma parte adicional do conteúdo de áudio/ vídeo criptografado (AVE).

2. Método, de acordo com a reivindicação 1, **caracterizado pelo** fato de que inclui ainda a etapa de:

- receber, pelo módulo de segurança (SM), uma mensagem de gerenciamento (EMM), compreendendo um comando para ativar/desativar a seleção de uma das duas palavras de controle (CW1, CW2, CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n).

3. Método, de acordo com a reivindicação 1 ou 2, **caracterizado pelo** fato de que ainda compreende a etapa de:

- receber, pelo módulo de segurança (SM), uma mensagem de gerenciamento (EMM), compreendendo um comando para forçar a seleção de uma das duas palavras de controle (CW1, CW2, CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n).

4. Método, de acordo com a reivindicação 2 ou 3, **caracterizado pelo** fato de que a mensagem de gerenciamento (EMM) compreende ainda uma indicação de um momento em que o comando deve ser executado.

5. Método, de acordo com qualquer uma das reivindicações 1 a 4, **caracterizado pelo** fato de que a etapa de conversão inclui ainda as etapas de:

- converter a palavra de controle selecionada (CW1, CW2, CW1a, CW2a, CW1b, CW2b, ..., CW1n, CW2n) para uma palavra de controle intermediária (CWI) por uma segunda função criptográfica (F) sob uma chave intermediária (KI);

- dividir a palavra de controle intermediária (CWI) em uma primeira parte (CWI1) e uma segunda parte (CWI2);

- aplicar a primeira função criptográfica (H) na primeira parte (CWI1) para obter uma palavra de controle parcial (CWP), esta palavra de controle parcial (CWP), sendo a mesma para uma primeira parte obtida a partir de qualquer uma das pelo menos

duas palavras de controle diferentes (CW1, CW2);

- concatenar (CONC) a palavra controle parcial (CWP) com a segunda parte (CWI2) para formar a palavra de controle final (CW).

6. Método, de acordo com qualquer uma das reivindicações 1 a 4, **caracterizado pelo** fato de que a primeira função criptográfica (H) é uma função de uma única via.

7. Método para identificar um módulo de segurança (SM) adaptado para realizar o método, conforme definido em qualquer uma das reivindicações de 1 a 6, o referido módulo de segurança (SM) compreendendo pelo menos uma configuração interna que permite que o módulo de segurança (SM) seja identificado com exclusividade (UA), o referido método **caracterizado pelo** fato de que compreende as etapas de:

- enviar pelo menos duas palavras de controle (CW1, CW2) de um operador (OP) para o módulo de segurança (SM);

- receber, por parte do operador (OP), pelo menos uma palavra de controle (CW1, CW2);

- determinar pelo menos uma primeira parte (UA1) da configuração interna (UA) pelo operador (OP), a referida determinação com base em uma correspondência da palavra de controle recebida (CW1, CW2) com uma das palavras de controle enviadas (CW1, CW2);

- enviar pelo menos um conjunto adicional de pelo menos duas palavras de controle (CW1a, CW2a) do operador (OP) para o módulo de segurança (SM);

- adicionalmente receber, pelo operador (OP), pelo menos

uma palavra de controle adicional (CW1a, CW2a);

- determinar pelo menos uma segunda parte (UA2) da configuração interna (UA) pelo operador (OP), a referida determinação com base em uma correspondência da palavra de controle adicional recebida (CW1a, CW2a) com uma das palavras de controle adicionais enviadas (CW1a, CW2a);

- reconstruir a configuração interna pelo operador (OP), a referida reconstrução com base pelo menos na primeira parte determinada (UA1) e na parte adicional determinada (UA2) da configuração interna (UA);

- usar o parâmetro de reconstrução para identificar o módulo de segurança (SM).

8. Dispositivo decodificador (DEC) para decriptografar conteúdo de áudio/vídeo criptografado (AVE), o referido dispositivo decodificador (DEC) **caracterizado pelo** fato de que compreende um desembaralhador (DESC) e um módulo de segurança (SM), o referido módulo de segurança com uma configuração interna (UA) e sendo configurado para:

- receber pelo menos um primeiro conjunto de pelo menos duas palavras de controle (CW1, CW2);

- selecionar um do primeiro conjunto de pelo menos duas palavras de controle, a referida seleção sendo feita com base em pelo menos uma primeira parte (UA1) da configuração interna (UA);

- passar a palavra controle selecionada para o desembaralhador (DESC);

- receber um conjunto adicional de pelo menos duas

palavras de controle (CW1a, CW2a);

- adicionalmente selecionar um do conjunto adicional de pelo menos duas palavras de controle, a referida seleção com base em pelo menos uma segunda parte (UA2) da configuração interna (UA); e

- passar a palavra controle selecionada adicional para o desembaralhador (DESC);

o referido desembaralhador (DESC) compreendendo pelo menos um módulo de decriptografia (DECR) para decriptografar o conteúdo de vídeo/ áudio criptografado (AVE), o desembaralhador (DESC) compreendendo ainda meios para realizar pelo menos uma primeira função criptográfica (H) e em que:

- os referidos meios para executar a primeira função criptográfica (H) convertem a palavra de controle selecionada (CW1, CW2) em uma primeira palavra de controle final e convertem a palavra de controle selecionada adicional (CW1a, CW2a) em uma palavra de controle adicional final, a referida função criptográfica (H) produzindo a mesma palavra de controle final (CW) para pelo menos as duas palavras de controle selecionadas e as mesmas palavras de controle adicionais finais para pelo menos as duas palavras de controle selecionadas adicionais;

- o referido desembaralhador compreende ainda meios para decriptografar (DECR) pelo menos uma parte do conteúdo de vídeo/ áudio codificado (AVE), usando a palavra de controle final (CW) e pelo menos uma parte adicional do conteúdo de áudio/vídeo criptografado (AVE) usando a palavra de controle

final adicional.

9. Dispositivo decodificador (DEC), de acordo com a reivindicação 8, **caracterizado pelo** fato de que o referido desembaralhador (DESC) inclui ainda:

- meios para realizar uma segunda função criptográfica (F), os referidos meios para realizar a segunda função criptográfica (F) sendo configurados para converter a palavra de controle selecionada (CW1, CW2) em uma palavra de controle intermediária (CWI) sob uma chave intermediária (KI);

- meios para dividir a palavra de controle intermediária (CWI) em uma primeira parte (CWI1) e uma segunda parte (CWI2);

em que os referidos meios para executar a primeira função criptográfica (H) convertem a primeira parte (CWI1) para uma palavra de controle parcial (CWP), esta palavra de controle parcial (CWP), sendo a mesma para uma primeira parte (CWI1) obtida a partir de qualquer uma das menos pelo menos duas palavras de controle diferentes (CW1, CW2) e em que o referido desembaralhador (DESC) compreende ainda meios para concatenar a palavra controle parcial (CWP) com a segunda parte (CWI2) para formar a palavra de controle final (CW).

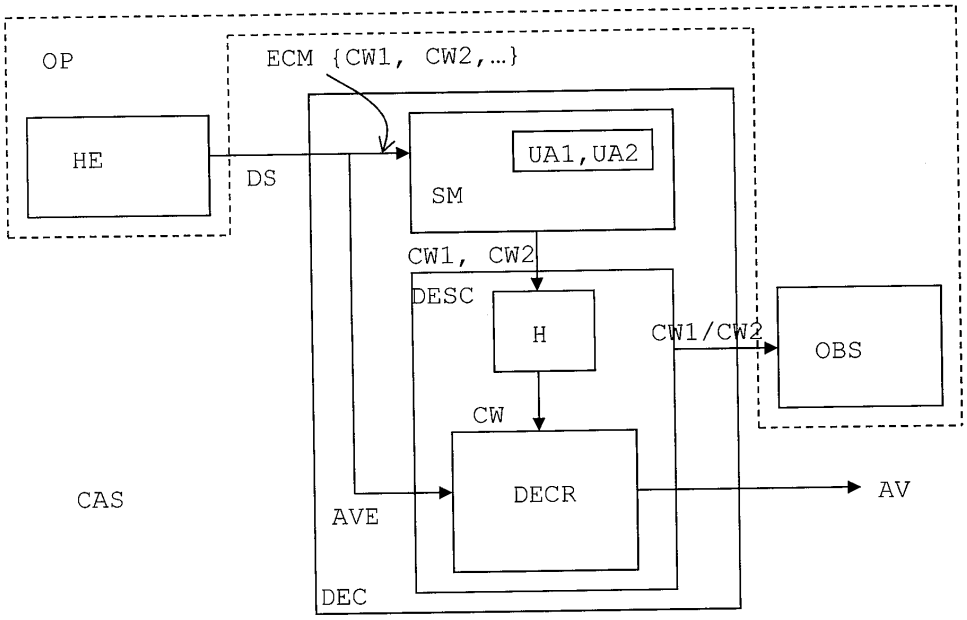
OP
ECM {CW1, CW2,…}
HE
DS
UA1,UA2
SM
CW1, CW2
DESC
H
CW1/CW2
OBS
CW
CAS
DECR
AV
AVE
DEC

Fig. 1

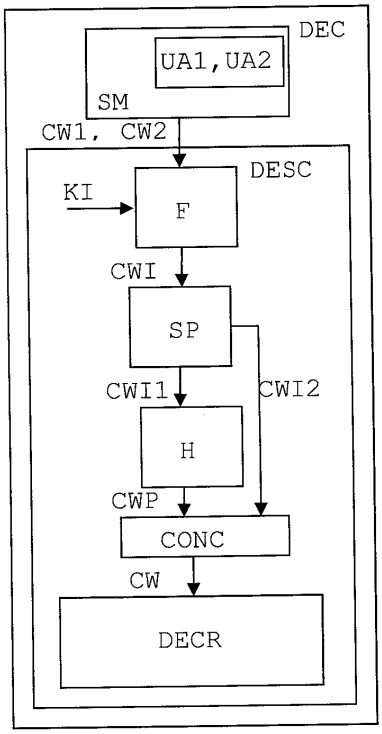
DEC
UA1,UA2
SM
CW1, CW2
DESC
KI
F
CWI
SP
CWI1
CWI2
H
CWP
CONC
CW
DECR

Fig. 2