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

(21) PI 0715101-2 A2

(22) Data de Depósito: 27/07/2007
(43) Data da Publicação: 04/06/2013
(RPI 2213)

(51) Int.Cl.:
H04L 9/08
G06F 21/24
G06Q 30/00

(54) Título: DISPOSITIVO TERMINAL, DISPOSITIVO SERVIDOR, E SISTEMA DE DISTRIBUIÇÃO DE CONTEÚDO

(30) Prioridade Unionista: 27/07/2006 JP 2006-205271

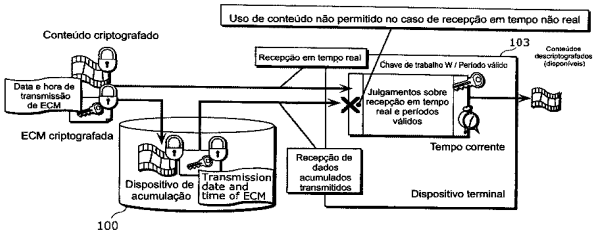
(73) Titular(es): Panasonic Corporation

(72) Inventor(es): Akio Higashi, Hiroki Murakami, Katsumi Tokuda, Ryuichi Okamoto

(86) Pedido Internacional: PCT JP2007064820 de 27/07/2007

(87) Publicação Internacional: WO 2008/013287de 31/01/2008

(57) Resumo: DISPOSITIVO TERMINAL, DISPOSITIVO SERVIDOR, E SISTEMA DE DISTRIBUIÇÃO DE CONTEÚDO. A fim de prover um sistema de distribuição de conteúdo que possa impedir o uso de um conteúdo que foi temporariamente acumulado após o período válido. Um sistema de distribuição de conteúdo (1) incluindo um servidor de licenciamento (101) que emite um licenciamento, um servidor de conteúdo (102) que transmite o conteúdo, um dispositivo terminal (103) que controla o uso do conteúdo com base no licenciamento emitido. O dispositivo terminal (103) não permite o uso do conteúdo criptografado recebido quando é julgado que o conteúdo criptografado recebido do servidor de conteúdo (102) não é o conteúdo recebido em tempo real.



Relatório Descritivo da Patente de Invenção para **"DISPOSITIVO TERMINAL, DISPOSITIVO SERVIDOR, E SISTEMA DE DISTRIBUIÇÃO DE CONTEÚDO".**

Campo da Técnica

A presente invenção refere-se a um sistema de distribuição de conteúdo para distribuir um conteúdo digital, tal como vídeo e música, através de uma rede, e, em particular, a um dispositivo servidor que distribui o conteúdo digital e chaves de descriptografia para o conteúdo digital, e a um dispositivo terminal que usa o conteúdo digital por meio do uso das chaves de descriptografia.

Fundamentos da Invenção

Recentemente, foram desenvolvidos sistemas chamados "sistemas de distribuição de conteúdo". Cada um dos "sistemas de distribuição de conteúdo" torna possível se distribuir um conteúdo digital (doravante simplesmente referido como "conteúdo"), como, por exemplo, música, vídeo, jogos, ou coisa do gênero a partir de um dispositivo servidor para um dispositivo terminal por meio de uma comunicação, tal como a Internet ou difusão digital, e usar o conteúdo no dispositivo terminal. Em um sistema de distribuição geral de conteúdo, é usada uma técnica de proteção de direito autoral no sentido de proteger o direito autoral do conteúdo e impedir que usuário malicioso utilize o conteúdo de uma forma não autorizada. Em termos mais específicos, esta "técnica de proteção de direito autoral" vem a ser uma técnica para o controle seguro do uso do conteúdo por meio da utilização de uma técnica de criptografia ou coisa do gênero.

Por exemplo, a difusão paga emprega um método de controle de misturação de acordo com o qual um sinal de vídeo e um sinal de áudio são misturados e transmitidos, e apenas os terminais tendo direito de visualização desmituram os sinais de vídeo e de áudio a fim de permitir a visualização do conteúdo.

Os detalhes do método de controle de misturação convencional acima mencionado são apresentados no Documento de Referência Não Patente 1 e no Documento de Referência Não Patente 2.

O método de controle de misturação convencional utiliza dois tipos de itens de informação chamados informação individual e informação de programa (doravante referidos na presente invenção como "informações relativas a conteúdo"). A informação individual vem a ser a informação que indica um contrato de visualização feito para cada um dos receptores, e inclui uma chave de trabalho que é requerida para descriptografar os contratos, os períodos válidos dos contratos, e os itens de informação relativa a conteúdo a serem transmitidos dali em diante. A informação relativa a conteúdo vem a ser a informação a ser transmitido em paralelo aos sinais de vídeo e de áudio misturados ou coisa do gênero, e inclui uma chave de misturação necessária para desmisturar estes sinais, o tempo corrente que indica o momento, e os detalhes do programa.

O dispositivo terminal que recebe o conteúdo recebe a informação individual endereçada ao próprio terminal e exibe os detalhes coma informação de contrato antes da recepção da informação relativa a conteúdo. Na visualização do programa, o dispositivo terminal recebe a informação relativa a conteúdo juntamente com os sinais de áudio e vídeo, verifica o tempo corrente e o período válido do contrato, incluídos na informação relativa a conteúdo, e verifica se o contrato expirou ou não. No caso em que o conteúdo tenha expirado, o dispositivo terminal julga o conteúdo como "Sem direito de visualização". No caso em que o conteúdo não tenha expirado, o dispositivo terminal verifica a presença/ausência de um direito de visualização verificando os detalhes do programa e os detalhes de contrato. No presente caso, somente quando o julgamento mostra que "existe direito de visualização", o dispositivo terminal extrai a chave de misturação e desmistura os sinais de áudio e vídeo ou coisa do gênero.

Desta maneira, o método de controle de misturação convencional faz um julgamento sobre o período válido de um contrato baseado no tempo corrente, que é transmitido juntamente com o conteúdo.

Documento de Referência Não Patente 1

Pedido N. 17 para recomendação do Conselho de Tecnologia de Telecomunicações, *Showa* 63 (1988), *Eisei housou ni yoru television housou*

ni okeru yuryo housiki ni kansuru gijutsu teki joken (Condições técnicas para o esquema pago em uma difusão de televisão via satélite)

Documento de Referência Não Patente 2

Pedido N. 74 para recomendação parcial do Conselho de Tecnologia de Telecomunicações,, Heisei 7 (1995), *Digital housou houshiki ni kakaru gijutsu teki joken* (Condições técnicas para um esquema de difusão digital)

Apresentação da Invenção

Problemas a serem Solucionados pela Invenção

No entanto, um dispositivo terminal que recebe um conteúdo distribuído nem sempre recebe uma informação relativa a conteúdo que será transmitida juntamente com o conteúdo imediatamente após a transmissão. Por exemplo, conforme mostrado na figura 1, é concebível que um usuário temporariamente armazene o conteúdo e a informação relativa a conteúdo que é transmitida juntamente com o conteúdo em um dispositivo de acumulação 100 ou coisa do gênero, e re-transmita os mesmos para o dispositivo terminal 1030 em um outro dia. Neste caso, o tempo no qual o dispositivo terminal 1030 recebe o conteúdo e a informação relativa a conteúdo é diferente do tempo corrente incluído na informação relativa a conteúdo. Sendo assim, de acordo com o método convencional, pode ser julgado se um contrato ainda não expirou, embora o contrato tenha de fato expirado. Além disso, no case em que o conteúdo e a informação relativa a conteúdo foram repetidamente re-transmitidos, o dispositivo terminal 1030 poderá permitir o uso do conteúdo repetidas vezes, a cada momento de uma re-transmissão. Além disso, é necessário que o tempo corrente ou coisa do gênero incluído na informação relativa a conteúdo não seja manipulado no sentido de realizar um processamento, como, por exemplo, a realização de um julgamento sobre um período válido. Além disso, o dispositivo terminal 1030 precisa verificar a integridade da informação relativa a conteúdo recebida. Este processamento é feito durante um intervalo de decodificação de um conteúdo, e, assim, a carga de processamento para este processo pode ser pequeno.

A presente invenção foi pensada considerando os problemas a-

cima mencionados, e tem um primeiro objeto de prover um sistema de distribuição de conteúdo ou coisa do gênero que torne possível se impedir que um usuário utilize um conteúdo expirado ao armazenar temporariamente o conteúdo.

Além do objeto acima descrito, a presente invenção tem um segundo objeto de prover um sistema de distribuição de conteúdo ou coisa do gênero que torne possível se verificar a integridade da informação relativa a conteúdo de acordo com um método que requeria uma pequena carga de processamento.

Maneiras de se solucionar os problemas

A fim de chegar aos objetos acima descritos, o dispositivo terminal de acordo com a presente invenção vem a ser um dispositivo terminal em um sistema de distribuição de conteúdo incluindo um dispositivo servidor e um dispositivo terminal, e o dispositivo terminal inclui: uma unidade de recebimento configurada para receber, do dispositivo servidor, (I) um conteúdo criptografado, e (II) uma informação relativa a conteúdo incluindo (II-i) informações de data e hora de transmissão e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo a fim de descriptografar o conteúdo criptografado; uma unidade de obtenção de informação de tempo configurada de modo a obter uma informação de data e hora correntes que indica a data e a hora correntes; uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e a hora indicada pelas informações de data e hora de transmissão recai dentro de uma faixa predeterminada; e uma unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a unidade de julgamento de recepção em tempo real julga que o conteúdo não está sendo recebido em tempo real.

Além disso, o dispositivo servidor, de acordo com a presente invenção, vem a ser um dispositivo servidor em um sistema de distribuição de conteúdo incluindo um dispositivo servidor e um dispositivo terminal, o dispositivo servidor inclui: uma unidade de transmissão configurada para transmitir um conteúdo criptografado e uma informação relativa a conteúdo incluindo

informações de data e hora de transmissão de um conteúdo criptografado e uma pluralidade de chaves de descriptografia de conteúdo a fim de descriptografar um conteúdo criptografado; uma unidade de geração de informação relacionada configurada para gerar, em uma informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo de modo a descriptografar o conteúdo criptografado; uma unidade de identificação de data e hora de transmissão configurada para gerar, em uma informação relativa a conteúdo, informações de data e hora de transmissão, cada qual indicando uma data e hora na qual uma informação relativa a conteúdo é transmitida; e uma unidade de criptografia de informação relacionada configurada para criptografar, em um modo de Encadeamento de Blocos Cifrados (CBC), uma informação relativa a conteúdo na qual a pluralidade de chaves de descriptografia de conteúdo e informações de data e hora de transmissão foram geradas, em que a unidade de geração de informação relacionada é configurada para gerar, em uma informação relativa a conteúdo, uma pluralidade de chaves de descriptografia de conteúdo, e a unidade de identificação de data e hora de transmissão é configurada para gerar informações de data e hora de transmissão, cada qual indicando a mesma data e hora em um bloco de criptografia imediatamente antes de um bloco de criptografia para uma chave correspondente dentre uma pluralidade de chaves de descriptografia de conteúdo.

Além disso, um dispositivo de geração de informação relativa a conteúdo, de acordo com a presente invenção, vem a ser um dispositivo de geração de informação relativa a conteúdo que gera a informação relativa a conteúdo a ser transmitida juntamente com um conteúdo criptografado, um dispositivo de geração de informação relativa a conteúdo inclui: uma unidade de geração de informação relacionada configurada para gerar, em uma informação relativa a conteúdo, uma pluralidade de chaves de descriptografia de conteúdo de modo a descriptografar um conteúdo criptografado; uma unidade de definição de data e hora de transmissão configurada para gerar, em uma informação relativa a conteúdo, informações de data e hora de transmissão, cada qual indicando uma data e hora em que uma informação relativa a conteúdo é transmitida; e uma unidade de criptografia de informa-

ção relacionada configurada de modo a criptografar, em modo de Encadeamento de Blocos Cifrados (CBC), uma informação relativa a conteúdo na qual uma pluralidade de chaves de descriptografia de conteúdo e informações de data e hora de transmissão foram geradas, em que a unidade de geração de informação relacionada é configurada de modo a gerar, em uma informação relativa a conteúdo, uma pluralidade de chaves de descriptografia de conteúdo, e uma unidade de identificação de data e hora de transmissão é configurada de modo a gerar informações de data e hora de transmissão, cada qual indicando uma mesma data e hora em um bloco de criptografia imediatamente antes de um bloco de criptografia para uma chave correspondente dentre uma pluralidade de chaves de descriptografia de conteúdo.

Deve-se notar que a presente invenção pode ser implementada como um método de uso de conteúdo ou método de geração de informação relacionado tendo as etapas correspondentes às unidades estruturais únicas do dispositivo terminal ou do dispositivo servidor, como um circuito integrado, e um programa que faz com que um computador execute estas etapas de método. Como uma questão de evidência, a presente invenção pode ser amplamente distribuída através de meios de gravação, tais como, DVD e/ou meios de transmissão media, tais como a Internet.

Além disso, a presente invenção pode ser implementada como um sistema de distribuição de conteúdo incluindo um dispositivo terminal e um servidor.

Efeitos da Invenção

De acordo com a presente invenção, torna-se possível prover um sistema de distribuição de conteúdo que permita o uso do conteúdo somente quando o conteúdo e a informação relativa a conteúdo são recebidos imediatamente após uma transmissão por parte de um provedor.

Além disso, de acordo com a presente invenção, é possível se verificar a integridade de uma informação relativa a conteúdo por meio da execução de um processo de descriptografia na informação relativa a conteúdo em um modo convencional de Encadeamento de Blocos Cifrados (CBC) e de um processo de comparação das informações descriptografadas com

as correspondentes informações criptografadas sem realizar um processamento tal como um cálculo de valor de sinal numérico, que requer uma grande carga de processamento e um processo especial de descriptografia não utilizando o modo de encadeamento CBC.

Breve Descrição dos Desenhos

A figura 1 é um diagrama para a ilustração de um problema em um sistema de distribuição de conteúdo convencional.

A figura 2 é um diagrama em blocos mostrando uma estrutura geral do sistema de distribuição de conteúdo de acordo com a presente invenção.

A figura é um diagrama em blocos mostrando o perfil de um sistema de distribuição de conteúdo de acordo com a presente invenção.

A figura 4 é um diagrama mostrando um esquema de criptografia executado no conteúdo do sistema de distribuição de conteúdo de acordo com a presente invenção.

A figura 5 é um diagrama mostrando a estrutura funcional de um servidor de licenciamento de acordo com a presente invenção.

A figura 6 é um diagrama mostrando um exemplar de um licenciamento gerado por uma unidade de geração de licenciamento do servidor de licenciamento de acordo com a presente invenção.

A figura 7 é um diagrama em blocos mostrando a estrutura funcional de servidor de conteúdo de acordo com a presente invenção.

As Figuras 8(a) e (b) são diagramas que mostram um exemplo de uma mensagem ECM de acordo com a presente invenção.

A figura 9 é um diagrama mostrando a disposição de dados de porções de criptografia de uma mensagem ECM de acordo com a presente invenção.

A figura 10 é um diagrama mostrando um procedimento de um processo de julgamento de detalhes de contrato realizado com base em um código de contrato e em um código de julgamento de contrato de acordo com a presente invenção.

A figura 11 é um diagrama em blocos mostrando a estrutura de

um dispositivo terminal de acordo com a presente invenção.

A figura 12 é um fluxograma de operações realizadas em uma transmissão e recepção de licenciamento de acordo com a presente invenção.

A figura 13 é um fluxograma das operações realizadas em um processo de transmissão de conteúdo de acordo com a presente invenção.

A figura 14 é um fluxograma das operações realizadas em um processo de recepção de conteúdo de acordo com a presente invenção.

A figura 15 é um fluxograma das operações realizadas em um Processo de julgamento de mensagem ECM de acordo com a presente invenção.

A figura 16 é um fluxograma das operações realizadas em um processo de julgamento de recepção em tempo real de acordo com a presente invenção.

A figura 17 é um fluxograma das operações realizadas em um processo de detecção de manipulação de acordo com a presente invenção.

A figura 18 é um fluxograma das operações realizadas em um processo de julgamento de detalhes de contrato de acordo com a presente invenção.

Referências Numéricas

100	-	Dispositivo de acumulação
101	-	Servidor de licenciamento
102	-	Servidor de conteúdo
103	-	Dispositivo terminal
104	-	Meio de transmissão
201	-	Chave de misturação Ks
203, 401	-	Chave de trabalho Kw
205	-	Chave de sessão Kse
220	-	ECM
230	-	Licenciamento
301, 503	-	Unidade de acumulação de chaves de trabalho
302	-	unidade de acumulação de informações de contrato
303, 902	-	Unidade de gerenciamento de informação única

304 - Unidade de geração de licenciamento
305 - Unidade de transmissão de licenciamento
402, 602 - ID de chave de trabalho
403 - Código de contrato
404 - Data e hora de partida
405 - Data e hora de finalização
406 - Informação de controle de saída
501 - Unidade de acumulação de conteúdo
502 -Unidade de acumulação de informações de atributos de conteúdo
504 - Unidade de codificação de conteúdo
505 - Unidade de geração de misturação de chaves
506 - Unidade de criptografia de conteúdo
507 - Unidade de identificação de data e hora de transmissão
508 - Unidade de geração de informação relacionada
509 - Unidade de criptografia de informação relacionada
510 - Unidade de multiplexação
511 - Unidade de transmissão
601 - Versão de formato
603 - Data e hora de transmissão
604 - Código de julgamento de contrato
605 - Dados privativos
606 - Chave de misturação (ímpar)
607 - Chave de misturação (par)
615 - Informação de controle de saída
901 - Unidade de armazenamento de licenciamento
903 - Unidade de recebimento de licenciamento
904 - Unidade de gerenciamento de licenciamento
905 - Unidade de recebimento de conteúdo
906 - Unidade de desmultiplexação
907 - Unidade de obtenção de informação de hora
908 - Unidade de descriptografia de informação relacionada
909 - Unidade de julgamento de recepção em tempo real

910 - Unidade de detecção de manipulação
911 - Unidade de julgamento de detalhes de contrato
912 - Unidade de controle de uso de conteúdo
913 - Unidade de controle de armazenamento de conteúdo
1030 - Dispositivo terminal

Melhor Modo de se Executar a Invenção

Uma modalidade de acordo com a presente invenção é descrita abaixo com referência aos desenhos. A presente invenção é descrita usando a modalidade e os desenhos em anexo a seguir, devendo-se notar, porém, que tais descrições são concebidas como exemplares e, deste modo, não são concebidas no sentido de limitar a presente invenção.

A figura 2 é um diagrama mostrando a estrutura geral do sistema de distribuição de conteúdo 1 de acordo com a presente invenção.

Na figura 2, o sistema de distribuição de conteúdo 1 inclui um servidor de licenciamento 101, um servidor de conteúdo 102, vários dispositivos terminais 103, e um meio de transmissão 104. Cada um dos elementos estruturais do sistema de distribuição de conteúdo 1 é descrito a seguir.

O servidor de licenciamento 101 é disposto ao lado de um provedor α, e é concebido para gerenciar o contrato (com relação ao direito de uso de conteúdo) feito para um usuário β e distribuir, para um dispositivo terminal 103, o licenciamento incluindo a informação relacionada ao contrato (informação de contrato) para o usuário β. Quando o licenciamento é distribuído a partir do servidor de licenciamento 101 para o dispositivo terminal 103, este licenciamento é seguramente distribuído através de um canal autenticado seguro (doravante referido como "SAC"). Por exemplo, uma SSL (Camada Segura de Soquete) pode ser usada como um canal SAC. Deve-se notar que cada um dos elementos estruturais de um licenciamento é descrito em detalhe mais adiante com referência aos desenhos.

O servidor de conteúdo 102 é disposto no provedor α, e é concebido no sentido de distribuir um conteúdo criptografado para o dispositivo terminal 103. É empregado como o formato do conteúdo distribuído pelo servidor de conteúdo 102 um fluxo de transporte (doravante referido como

TS) definido nos Sistemas do padrão MPEG-2 (Moving Picture Expert Group 2) (Grupo de Especialistas em Imagem em Movimento (IEC/ISO13818-1), ou coisa do gênero.

O dispositivo terminal 103 é disposto no usuário β, e é concebido para usar o conteúdo distribuído a partir do servidor de conteúdo 102 através do uso do licenciamento distribuído a partir do servidor de licenciamento 101.

Exemplos de um meio de transmissão 104 incluem a Internet, os meios de comunicação com fio ou os meios de comunicação sem fio, como, por exemplo, uma CATV (Televisão a Cabo) e é ondas largas, além dos meios portáteis de gravação. O meio de transmissão 104 é concebido para conectar o servidor de licenciamento 101, o servidor de conteúdo 102, e os dispositivos terminais 103 de modo que os mesmos possam trocar dados.

Deve-se notar que a figura 3 é um diagrama em blocos mostrando o perfil de um sistema de distribuição de conteúdo 1 de acordo com a presente invenção. Conforme mostrado na figura 3, o sistema de distribuição de conteúdo 1 principalmente permite o uso de um conteúdo somente quando o tempo de recepção de um conteúdo é aproximadamente igual ao tempo de distribuição do conteúdo criptografado e de uma mensagem ECM criptografada a partir do dispositivo servidor de distribuição (tal recepção sendo chamada de "recepção em tempo real") e quando o contrato para o conteúdo ainda não expirou. O sistema de distribuição de conteúdo 1 não permite o uso do conteúdo quando o conteúdo é temporariamente acumulado no dispositivo de acumulação 100 e, deste modo, o mesmo é recebido em tempo real. Neste caso, quando a diferença entre o tempo de distribuição e o tempo de recepção é de, por exemplo, "dentro de 30 minutos", tal recepção pode ser chamada de "recepção em tempo real".

Foi feita acima uma descrição de uma estrutura geral de um sistema de distribuição de conteúdo 1 da presente modalidade. Com referência à figura 4, a descrição a seguir nesta modalidade é de um esquema de criptografia realizado no conteúdo a ser distribuído no sistema de distribuição de conteúdo 1.

O provedor α e o usuário β na figura 4 são descritos separadamente. O provedor α transmite o conteúdo criptografado e uma chave de criptografia para descriptografar o conteúdo criptografado, enquanto o usuário β recebe o conteúdo criptografado e a chave de criptografia.

Pelo lado do provedor α, o conteúdo 200 é misturado (ou seja, criptografado) por meio do uso de uma chave de criptografia chamada a chave de misturação Ks 201 (S202). Em uma misturação, é cargas úteis dos pacotes de fluxo TS do padrão MPEG-2 são misturadas em uma base de pacote de fluxo TS. Deve-se notar que esta chave de misturação Ks 201 é uma chave variável no tempo que é alterada em uma freqüência, por exemplo, variando de poucos segundos a alguns dias a fim de aumentar a segurança contra uma recepção não autorizada.

A chave de misturação Ks 201 para a criptografia do conteúdo 200 é criptografada (S204) por meio do uso de uma chave de trabalho KW 203 a fim de impedir a interceptação não autorizada realizada por um usuário malicioso. A chave de trabalho Kw 203 é uma chave de criptografia atribuída a uma base de um provedor, um contrato, um grupo, ou coisa do gênero de modo que a mesma possa ser usada de acordo com um método de recepção limitado geral convencional, e, em geral, a mesma é atualizada após um período que varia de um mês a alguns anos a fim de garantir a segurança da própria chave de trabalho Kw 203. A chave de trabalho Kw 203 inclui pelo menos a chave de misturação Ks 201. A estrutura de dados para a transmissão de uma informação relativa a conteúdo é chamada ECM (Entitlement Control Message) (Mensagem de Controle de Titularidade) 220 estruturada como seções privadas definidas nos Sistemas de padrão MPEG-2. Deve-se notar que um exemplo de uma estrutura de dados desta mensagem ECM 220 será descrita em detalhe a seguir com referência aos desenhos.

A chave de trabalho Kw 203 que criptografa a mensagem ECM 220 incluindo a chave de misturação Ks 201 devem ser compartilhadas entre o provedor α e o usuário β antes do uso de um conteúdo. Conforme mostrado na figura 4, tal compartilhamento é obtido ao se gera uma chave de trabalho criptografada Kw 203 no licenciamento 230 e ao se distribuir o licencia-

mento 230 a partir do provedor α para o usuário β através de um canal SAC. Em termos mais específicos, a chave de sessão Kse 205 é compartilhada entre os mesmos quando um canal SAC é estabelecido entre o provedor α e o usuário β, e, desta forma, o provedor α criptografa (S206) o licenciamento 230 por meio do uso de uma chave de sessão Kse 205.

Deve-se notar que um método de criptografia de chave comum, como, por exemplo, o AES (FIPS-197) é geralmente usado como um algoritmo de criptografia utilizado neste esquema de criptografia.

O conteúdo criptografado gerado e a mensagem ECM 220 criptografada conforme descrito acima são convertidos em pacotes de fluxo TS no padrão MPEG-2, multiplexados (S207) com dados, por exemplo, com informações PSI (Program Specific Information) (Informação Específica de Programa)/SI (Serviço Information) (Informação de Serviço) ou coisa do gênero, conforme necessário, e, em seguida, transmitidos ao usuário β.

Por outro lado, o usuário β recebe, antes do uso do conteúdo 200, um licenciamento 230 incluindo a chave de trabalho Kw 203 criptografada (S206) por meio do uso de uma chave de sessão Kse 205 no provedor α e, em seguida, transmitida, e descriptografa (S211) o licenciamento recebido por meio do uso de uma chave de sessão Kse 205 compartilhada com o provedor α através do canal SAC a fim de obter a chave de trabalho Kw 203.

Além disso, quando o usuário β recebe os pacotes de padrão MPEG-2 TS incluindo o conteúdo criptografado a partir do provedor α, o usuário β desmultiplexa (S212) os pacotes de fluxo TS de modo a obter o conteúdo criptografado 210, a mensagem ECM criptografada 220, ou coisa do gênero. Em seguida, o usuário β descriptografa (S213) a mensagem ECM criptografada 220 por meio do uso da chave de trabalho Kw 203 obtida a fim de obter a chave de misturação Ks 201. Neste momento, o usuário β obtém a chave de misturação Ks 201 da mensagem ECM 220, e faz um julgamento sobre a disponibilidade. Este processo de julgamento é descrito em detalhe a seguir com referência aos desenhos.

Em seguida, o usuário β desmistura (ou seja, descriptografa) (S214) o conteúdo criptografado 210 por meio do uso da chave de mistura-

ção Ks 201 obtida de modo que o usuário β possa usar (visualizar, gravar, ou coisa do gênero) o conteúdo.

A figura 5 é um diagrama em blocos mostrando a estrutura funcional do servidor de licenciamento 101 na presente modalidade. Na figura 5, o servidor de licenciamento 101 inclui uma unidade de acumulação de chaves de trabalho 301, uma unidade de acumulação de informações de contrato 302, uma unidade de gerenciamento de informação única 303, um unidade de geração de licenciamento 304, e uma unidade de transmissão de licenciamento 305. Estes respectivos elementos estruturais são descritos a seguir.

A unidade de acumulação de chaves de trabalho 301 é, por exemplo, uma memória RAM, e acumula a chave de trabalho Kw 203. Pressupõe-se que a unidade de acumulação de chaves de trabalho 301 acumule a chave de trabalho Kw 203 juntamente com um identificador que identifica unicamente a chave de trabalho Kw 203 dentro do sistema de distribuição de conteúdo 1, a data de partida de transmissão da chave de trabalho, ou coisa do gênero, e que o identificador identifique a chave de trabalho Kw 203 que deve ser transmitida para o dispositivo terminal 103.

A unidade de acumulação de informações de contrato 302 é usada para gerenciar a informação de contrato que é requerida por parte do usuário β que usa este sistema de distribuição de conteúdo no sentido de utilizar um conteúdo. Neste caso, exemplos de "informação de contrato" incluem informações para associar o usuário β e o dispositivo terminal 103, informações para identificar o serviço para o qual o usuário β fez um contrato, e informações que incluem o ponto de partida e o ponto de finalização de um período válido do contrato.

A unidade de gerenciamento de informação única 303 é, por exemplo, um microcomputador que inclui uma memória ROM ou coisa do gênero para o armazenamento de um programa de controle, e é usada para controlar é funções gerais de um servidor de licenciamento 101. Além disso, a unidade de gerenciamento de informação única 303 gerencia informações únicas de um servidor de licenciamento 101, e obtém informações únicas tal como uma chave secreta de um servidor de licenciamento 101 requerida

para estabelecer um canal SAC para o dispositivo terminal 103 e um certificado de chave pública de um servidor de licenciamento 101.

A unidade de geração de licenciamento 304 gera o licenciamento 230 a ser distribuído para um dispositivo terminal 103 em resposta a uma solicitação do dispositivo terminal 103.

A unidade de transmissão de licenciamento 305 estabelece o canal SAC para o dispositivo terminal 103, e transmite o licenciamento 230 gerado por uma unidade de geração de licenciamento 304 para o dispositivo terminal 103 em resposta a uma solicitação do dispositivo terminal 103.

Foi feita acima uma descrição de uma estrutura geral de um servidor de licenciamento 101 da presente modalidade.

A figura 6 é um diagrama mostrando um exemplo do licenciamento 230 gerado por uma unidade de geração de licenciamento 304 do servidor de licenciamento 101. Conforme mostrado na figura 6, o licenciamento 230 inclui uma chave de trabalho Kw 401, um identificador ID de chave de trabalho 402, um código de contrato 403, uma data e hora de partida 404, uma data e hora de finalização 405, e informações de controle de saída 406.

A chave de trabalho Kw 203 mostrada na figura 4 é gerada em uma chave de trabalho Kw 401. Deve-se notar que, quando a chave de trabalho Kw 203 é periodicamente atualizada, torna-se possível gerar uma chave de trabalho Kw 203 corrente e uma chave de trabalho Kw 203 como é chaves de trabalho Kw 401 do licenciamento 230. O identificador ID que identifica unicamente a chave de trabalho Kw 203 a ser gerada em uma chave de trabalho Kw 401 é gerado no identificador ID de chave de trabalho 402. Um código indicando os detalhes do contrato feito para o usuário β que usa o dispositivo terminal 103 é gerado em um código de contrato 403. Este código é também chamado de bits de nível. O ponto de partida no qual uma chave de trabalho Kw 401 pode ser usada é gerado em uma data e hora de partida 404. Em uma data e hora de finalização 405, o ponto de finalização no qual o direito de uso de uma chave de trabalho Kw 401 é perdido. Informações relativas às saídas digitais, ás saídas analógicas, à gravação em um

meio de gravação, tal como um meio removível, e o controle de acumulação no tempo em que um conteúdo é usado são geradas na informação de controle de saída 406. Exemplos de tais informações incluem a informação de controle de cópia analógico/digital (referida doravante como uma informação "CCI"),o sistema de proteção de cópia analógica, a criptografia EPN (criptografia mais não asserção), e a informação relativa à acumulação temporária. Exemplos específicos de tais informações a serem geradas como uma informação de controle de cópia incluem o "Copy never" ("Nunca copie"), o "Copy once" (Copiar uma vez"), o "Copy Free" ("Cópia livre") ou coisa do gênero.

Foi feita acima uma descrição de um licenciamento 230 da presente modalidade.

A figura 7 é um diagrama em blocos mostrando uma estrutura funcional de um servidor de conteúdo 102 na presente modalidade. Conforme mostrado na figura 7, o servidor de conteúdo 102 inclui uma unidade de acumulação de conteúdo 501, uma unidade de acumulação de informações de atributos de conteúdo 502, uma unidade de acumulação de chaves de trabalho 503, uma unidade de codificação de conteúdo 504, uma unidade de geração de misturação de chaves 505, uma unidade de criptografia de conteúdo 506, uma unidade de identificação de data e hora de transmissão 507, uma unidade de geração de informação relacionada 508, uma unidade de criptografia de informação relacionada 509, uma unidade de multiplexação 510, e uma unidade de transmissão 511.

A unidade de acumulação de conteúdo 501 vem a ser um dispositivo de disco rígido, um gravador de DVD, ou coisa do gênero, e acumula conteúdo. Além disso, pressupõe-se que um identificador para identificar unicamente um conteúdo dentro de um sistema de distribuição de conteúdo 1, um nome de conteúdo, uma data e hora de distribuição de um conteúdo, ou coisa do gênero são acumulados em uma unidade de acumulação de conteúdo 501.

A unidade de acumulação de informações de atributos de conteúdo 502 vem a ser uma memória RAM ou coisa do gênero, e acumula in-

formações relativas a um conteúdo. Além disso, pressupõe-se que um identificador para identificar unicamente um conteúdo dentro de um sistema de distribuição de conteúdo 1, informações que identificam o contrato necessário para usar conteúdo, ou coisa do gênero são acumulados em uma unidade de acumulação de informações de atributos de conteúdo 502.

A unidade de acumulação de chaves de trabalho 503 é, por exemplo, uma memória RAM, e acumula uma chave de criptografia a fim de criptografar uma mensagem ECM 220. Além disso, pressupõe-se que a unidade de acumulação de chaves de trabalho 503 acumula a chave de trabalho Kw 203 e o identificador ID de chave de trabalho 402 juntamente com a chave de trabalho utilizam uma data de partida ou coisa do gênero, e a chave de trabalho Kw 203 que deve ser aplicada a uma mensagem ECM 220 pode ser identificada de acordo com um tempo de transmissão.

A unidade de codificação de conteúdo 504 lê o conteúdo a ser transmitido para o dispositivo terminal 103 a partir de uma unidade de acumulação de conteúdo 501, e codifica o conteúdo em um formato de padrão MPEG. Além disso, a unidade de codificação de conteúdo 504 vem a ser um codificador em tempo real que gera um fluxo de padrão MPEG, e lê o vídeo, o áudio, ou coisa do gênero de uma unidade de acumulação de conteúdo 501 de acordo com uma instrução por parte de um sistema de fluxo ascendente (por exemplo, um sistema de gerenciamento de programação de programa), e gera um padrão MPEG-2 ou H. 264 ES (Elementary Stream) (Fluxo Elementar) incluindo o vídeo e o áudio. Além disso, a unidade de codificação de conteúdo 504 gera pacotes PES (Packetized Elementary Stream) (Fluxo Elementar Pacotizado) incluindo estes fluxos ES, converte os pacotes de fluxo PES em pacotes de padrão MPEG-2 TS, e, por último, transmite os pacotes de fluxo TS para uma unidade de multiplexação 510.

A unidade de geração de misturação de chaves 505 gera a chave de misturação Ks 201 a fim de misturar um conteúdo. Além disso, a unidade de geração de misturação de chaves 505 sequencialmente gera é chaves de misturação Ks 201 baseadas em um período de atualização das chaves de misturação Ks 201, e transmite é mesmas para uma unidade de crip-

tografia de conteúdo 506.

A unidade de criptografia de conteúdo 506 mistura o conteúdo. Além disso, a unidade de criptografia de conteúdo 506 criptografa (mistura) é cargas úteis dos pacotes de fluxo TS, por meio da chave de misturação Ks 201 obtida a partir de uma unidade de geração de misturação de chaves 505, ou de um método AES ou coisa do gênero, no modo CBC (encadeamento de blocos cifrados) mais o modo OFB (realimentação de saída).

A unidade de identificação de data e hora de transmissão 507 é, por exemplo, um microcomputador incluindo uma memória ROM para o armazenamento de um programa de controle, e controla é funções gerais de um servidor de conteúdo 102. Além disso, a unidade de identificação de data e hora de transmissão 507 vem a ser uma unidade para o gerenciamento de informações de tempo e provê o tempo corrente para uma unidade que requeira tal informação de tempo.

A unidade de geração de informação relacionada 508 gera, em uma informação relativa a conteúdo (ECM 220), é chaves de descriptografia de conteúdo (em particular, em um número plural) para a descriptografia do conteúdo criptografado. Em termos mais específicos, a unidade de geração de informação relacionada 508 gera uma mensagem ECM 220 incluindo a chave de misturação Ks 201 gerara em uma unidade de geração de misturação de chaves 505. Além disso, a unidade de geração de informação relacionada 508 gera uma mensagem ECM 220 de acordo com uma instrução do sistema de fluxo ascendente, os momentos de transmissão de um conteúdo e a obtenção de uma chave de misturação Ks 201 a partir de uma unidade de geração de misturação de chaves 505. A mensagem ECM 220 gerada é transmitida para uma unidade de multiplexação 510.

A unidade de criptografia de informação relacionada 509 criptografa a mensagem ECM 220 gerada por uma unidade de geração de informação relacionada 508. A unidade de criptografia de informação relacionada 509 recebe a mensagem ECM 220 de uma unidade de geração de informação relacionada 508, e criptografa a mensagem ECM 220 por meio do uso de uma chave de trabalho Kw 203 obtida a partir de uma unidade de acumu-

lação de chaves de trabalho 503. O método AES ou coisa do gênero, e o encadeamento CBC mais a realimentação OFB como o modo de criptografia são usados para criptografar uma mensagem ECM 220. Além disso, a unidade de criptografia de informação relacionada 509 transmite a mensagem ECM 220 criptografada desta maneira para uma unidade de multiplexação 510.

A unidade de multiplexação 510 multiplexa os fluxos TS incluindo o vídeo, o áudio, e os dados recebidos de uma unidade de criptografia de conteúdo 506 com os fluxos TS de uma mensagem ECM 220 recebida de uma unidade de criptografia de informação relacionada 509 a fim de gerar os fluxos TS multiplexados.

A unidade de transmissão 511 transmite os fluxos TS gerados por uma unidade de multiplexação 510 para o dispositivo terminal 103. Por exemplo, a unidade de transmissão de conteúdo 511 multidifunde os fluxos TS na rede IP (Internet Protocol) (Protocolo da Internet) a fim de transmitir os mesmos para o dispositivo terminal 103.

Na presente modalidade, é feita a descrição das funções gerais de um servidor de conteúdo 102.

A figura 8(a) é um diagrama mostrando um exemplo de uma mensagem ECM 220 gerada por uma unidade de geração de informação relacionada 508. Conforme mostrado na figura 8(a), a mensagem ECM 220 inclui uma versão de formato 601, um identificador ID de chave de trabalho 602, uma data e hora de transmissão 603, um código de julgamento de contrato 604, os dados privativos 605, uma chave de misturação (ímpar) 606, e uma chave de misturação (par) 607.

As informações para a identificação do formato de uma mensagem ECM 220 e o método de criptografia de uma mensagem ECM 220 é gerado em uma versão de formato 601.

As informações para a identificação de uma chave de trabalho Kw 203 para a criptografia de uma mensagem ECM 220 são geradas no identificador ID de chave de trabalho 602. O identificador ID de chave de trabalho 602 é gerado nas porções não criptografadas de uma mensagem ECM

220, e, deste modo, é possível se identificar a chave de trabalho Kw 203 que deve ser usada para descriptografar a mensagem ECM 220 criptografada pelo dispositivo terminal 103 por meio da referência ao identificador ID de chave de trabalho 602 ao se descriptografar a mensagem ECM 220. No identificador ID de chave de trabalho 602, um código que identifica o provedor do serviço, e informações que identificam o par de chaves de trabalho (par/ímpar) Kw 203 podem ser incluídas.

O tempo corrente obtido a partir de uma unidade de identificação de data e hora de transmissão 507 é gerado em uma data e hora de transmissão 603. Em outras palavras, a mensagem ECM 220 e a data e hora de transmissão do conteúdo são geradas em uma data e hora de transmissão 603.

O código de julgamento de contrato 604 vem a ser uma informação que indica o atributo de um conteúdo, e é usado para julgar se um contrato para a visualização do conteúdo foi feito em um tempo de visualização de conteúdo por meio do uso do dispositivo terminal 103.

Os dados privativos 605 vêm a ser um campo no qual um dado arbitrário pode ser gerado. Nesta modalidade, os dados privativos 605 são gerados como um enchimento para a obtenção de um alinhamento com o tamanho do bloco de criptografia. Deve-se notar que a informação de controle de saída 615 pode ser armazenada como uma porção de dados privativos 605 conforme mostrado na figura 8(b). Esta informação de controle de saída 615 possui a mesma estrutura de dados que a da informação de controle de saída 406 no licenciamento 230 da figura 6. Um valor igual ou diferente do da informação de controle de saída 406 pode ser gerado na mesma. Quando a informação de controle de saída 615 é gerada como uma porção dos dados privativos 605, sendo que uma dentre a informação de controle de saída 406 ou a informação de controle de saída 615 é priorizada e determinada de acordo com uma regra predeterminada. Nesta modalidade, pressupõe-se que o dispositivo terminal 103 basicamente prioriza a informação de controle de saída 615. Deve-se notar que a presente invenção não se limita a esta modalidade. Por exemplo, é adequado se referir a ambas, e aplicar uma das

mesmas que tenha menos limitações ou que tenha limitações menos severas em um caso no qual os valores sejam diferentes entre si.

A chave de misturação Ks 201 para a criptografia das cargas úteis dos pacotes de fluxo TS de um conteúdo é gerada em uma chave de misturação (ímpar) 606.

A chave de misturação Ks 201 para a criptografia das cargas úteis dos pacotes de fluxo TS de um conteúdo, da mesma forma que a chave de misturação (ímpar) 606, é gerada em uma chave de misturação (par) 607. A transmissão das chaves de misturação (ímpar/par) Ks 201 na mensagem ECM 220 permite que o dispositivo terminal 103 use continuamente o conteúdo par quando é chaves de misturação Ks 201 são comutadas.

Neste caso, a versão de formato 601 e o identificador ID de chave de trabalho 602 da mensagem ECM 220 sãos dados que não são criptografados, enquanto a data e hora de transmissão 603, o código de julgamento de contrato 604, os dados privativos 605, a chave de misturação (ímpar) 606, a chave de misturação (par) 607 sãos dados a serem criptografados por meio do uso do método AES em um modo de encadeamento CBC. Além disso, pressupõe-se que o modo de realimentação OFB seja usado de forma concorrente no momento de ocorrência de um número fracional menor que o tamanho de bloco de criptografia (por exemplo, 16 bytes em um método AES tendo um tamanho de chave de 128 bits). Pressupõe-se que um valor fixo seja usado como o valor de IV (vetor de inicialização) no modo de encadeamento CBC, e seja único para um dispositivo (não pode ser modificado de fora) pelo menos dentro do dispositivo terminal 103.

Neste caso, a disposição de dados das porções de criptografia em uma mensagem ECM 220 é descrita em mais detalhes com referência à figura 9.

A figura 9 é um diagrama mostrando os detalhes das porções de criptografia (as porções a serem criptografadas) de uma mensagem ECM 220 mostrada na figura 8, e uma data e hora de transmissão 603, um código de julgamento de contrato 604, e dados privativos 605 são gerados em cada um dos blocos de criptografia 1 a 3. A chave de misturação (ímpar) 606 é

gerada no bloco de criptografia 2, e a chave de misturação (par) 607 é gerada no bloco de criptografia 4 em um dado exemplo.

Os dados que devem ser protegidos contra a manipulação de um usuário não autorizado ou algo do gênero em uma mensagem ECM 220 são a data e hora de transmissão 603 e o código de julgamento de contrato 604 relativo ao julgamento, feito pelo dispositivo terminal 103, sobre a disponibilidade de conteúdo.

Com referência à figura 10A, é feita a descrição de um exemplo de um processo de julgamento de consistência realizado em cada bit por meio do uso do código de julgamento de contrato 604 de uma mensagem ECM 220 e o código de contrato 403 do licenciamento 230 no dispositivo terminal 103.

Conforme mostrado na figura 10, o código de julgamento de contrato 604 vem a ser uma disposição de bits (mapa de bits) na qual os serviços são associados aos bits um a um. O bit correspondente ao serviço que pertence ao conteúdo que inclui a mensagem ECM 220 é definido em "1", e os outros bits são definidos em "0". Por outro lado, em um código de contrato 403, os serviços são associados aos bits da mesma maneira. O bit correspondente ao serviço para o qual o usuário β fez um contrato é definido em "1", e "0" é definido para os serviços para os quais o usuário β não fez um contrato.

Quando o dispositivo terminal 103 recebe uma mensagem ECM 220, o mesmo calcula o produto lógico (AND) do código de julgamento de contrato 604 e do código de contrato 403. O dispositivo terminal 103 julga se "existe um contrato" quando o resultado mostra que qualquer um dos bits é "1", e julga como "sem contrato" quando o resultado mostra que todos os bits são "0".

O dispositivo terminal 103 realiza um processo de julgamento de detalhes de contrato com base no código de julgamento de contrato 604 da mensagem ECM 220 e no código de contrato 403 do licenciamento 230 por meio do uso de um método extremamente simples de um processo de julgamento de consistência realizado, desta maneira, em cada bit. Sendo as-

sim, no caso em que uma mensagem ECM 220 criptografada parcialmente manipulada é descriptografada, o valor do código de julgamento de contrato 604 fica diferente do valor devido que indica o contrato. Isto desabilita um julgamento corrente sobre os detalhes de contrato, o que poderá levar a um uso não autorizado do conteúdo. Da mesma forma, existe a possibilidade de um correto julgamento sobre os detalhes de contrato não poder ser feito com base em uma data e hora de transmissão 603 devido à manipulação da mensagem ECM criptografada 220, o que poderá levar a um uso não autorizado do conteúdo.

Por isso, na modalidade da figura 9, os dados incluídos na mensagem ECM 220 são protegidos contra manipulação por meio do uso do recurso de blocos de encadeamento em um modo de encadeamento CBC. Em outras palavras, o modo de encadeamento CBC é caracterizado pelo fato de que dois blocos criptografados adjacentes são encadeados na descriptografia, e, desta maneira, quando um bit específico de um determinado bloco de criptografia é invertido, a inversão poderá afetar todos os bits do bloco ou afetar apenas os bits correspondentes a um bloco de criptografia seguinte. Na figura 9, a data e hora de transmissão 603 e o código de julgamento de contrato 604 são substancialmente protegidos contra manipulação, uma vez que a obtenção de uma chave de misturação Ks 201 correta é desabilitada (em outras palavras, o conteúdo não poderá ser usado, uma vez que o conteúdo não poderá ser corretamente descriptografado) no caso da manipulação por meio de uma disposição de dados que cause dano por parte de uma pessoa não autorizada (na presente modalidade, a chave de misturação Ks 201 para a descriptografia do conteúdo) em um bloco posicionado próximo do bloco de criptografia que inclui dados que devem ser protegidos contra tal manipulação (na presente modalidade, a data e hora de transmissão 603 e um código de julgamento de contrato 604).

Além disso, o resultado da descriptografia do bloco de criptografia no qual uma inversão de bits foi realizada poderá afetar todos os bits de um bloco de criptografia, enquanto apenas um bit invertido será afetado em um bloco de criptografia seguinte. Considerando este fato, na figura 9, os

dados privativos 605 são dispostos de tal maneira que a chave de misturação Ks 201 fique alinhada no limite entre os blocos criptografados. Além disso, no caso da aplicação de um método AES tendo um tamanho de 128 bits como um algoritmo a ser aplicado ao conteúdo e à mensagem ECM 220, cada qual dentre o bloco de criptografia e a chave de misturação têm um tamanho de 16 bytes, e conforme mostrado na figura 8, o tamanho da chave de misturação Ks 201 é igual ao tamanho de um único bloco de criptografia. Deste modo, é possível se empregar uma estrutura que impeça que uma pessoa não autorizada obtenha um par corrente de chaves de misturação Ks 201 no caso de se inverter qualquer um dentre os bits de um bloco de criptografia imediatamente antes do bloco de uma chave de misturação Ks 201.

Além disso, uma vez que a mensagem ECM 220 inclui a chave de misturação (ímpar) 606, a chave de misturação (par) 607, e duas chaves de misturação Ks 201, existe a possibilidade de uma das chaves de misturação 201 corretas não poder ser obtida, enquanto uma outra poderá ser obtida no caso em que uma tentativa de manipulação for feita na data e hora de transmissão 603 e no código de julgamento de contrato 604 mesmo que o recurso de se encadear blocos no modo de encadeamento CBC seja simplesmente utilizado. Isto pode levar ao uso não autorizado do conteúdo. Por este motivo, na figura 9, a data e hora de transmissão 603 e o código de julgamento de contrato 604 são dispostos em cada um dentre o bloco de criptografia 1 e o bloco de criptografia 3, que vêm a ser os blocos de criptografia imediatamente precedentes ao bloco de criptografia 2 para uma chave de misturação (ímpar) 606, e o bloco de criptografia 4 para uma chave de misturação (par) 607 dispõe os blocos de criptografia 1 a 4 como uma seqüência de blocos de criptografia, e gera o mesmo valor para a data e hora de transmissão 603 e para o código de julgamento de contrato 604 de cada um dos blocos de criptografia 1 a 3. O dispositivo terminal 103 pode detectar uma manipulação mesmo quando pelo menos um dentre é datas e horas de transmissão 603 e os códigos de julgamento de contrato 604 foi manipulado, ao se julgar se é duas datas e horas de transmissão 603 são idênticas e os dois códigos de julgamento de contrato 604 da mensagem ECM descripto-

grafada 220 são idênticos. Além disso, um efeito vantajoso é provido ao se poder detectar uma manipulação antes do processo de obtenção da chave de misturação Ks 201 por meio do julgamento sobre a consistência dos dois códigos de julgamento de contrato 604.

Na presente modalidade, o uso da mensagem ECM 220 configurada conforme acima descrita elimina um processamento, como, por exemplo, a MIC (Message Integrity Check) (Verificação de Integridade de Mensagem), que requer uma grande quantidade de cálculos, e precisa apenas de um processo de criptografia e de um processo simples de julgamento de consistência de dados a fim de substancialmente impedir a manipulação de uma mensagem ECM 220. Não é necessário se usar um modo especial de criptografia ou coisa do gênero no processo de criptografia, e o modo de encadeamento CBC que é um modo padrão de criptografia poderá ser usado. Além disso, é necessário apenas se fazer um julgamento sobre a consistência de dados, que devem ser protegidos contra a manipulação dos blocos de criptografia (na presente modalidade, é datas e horas de transmissão 603, e os códigos de julgamento de contrato 604) do processo de julgamento de consistência de dados. Por conseguinte, é considerado que o esquema mostrado nesta modalidade pode ser facilmente implementado.

Nesta modalidade acima, foi feita a descrição de uma disposição de dados das porções de criptografia em uma mensagem ECM 220.

A figura 11 é um diagrama em blocos mostrando a estrutura funcional do dispositivo terminal 103 nesta modalidade. Conforme mostrado na figura 11, o dispositivo terminal 103 inclui uma unidade de armazenamento de licenciamento 901, uma unidade de gerenciamento de informação única 902, uma unidade de recebimento de licenciamento 903, uma unidade de gerenciamento de licenciamento 904, uma unidade de recebimento de conteúdo 905, uma unidade de desmultiplexação 906, uma unidade de obtenção de informação de hora 907, uma unidade de descriptografia de informação relacionada 908, uma unidade de julgamento de recepção em tempo real 909, uma unidade de detecção de manipulação 910, uma unidade de julgamento de detalhes de contrato 911, uma unidade de controle de uso de con-

teúdo 912, e uma unidade de controle de armazenamento de conteúdo 913. Os respectivos elementos estruturais são descritos abaixo.

A unidade de armazenamento de licenciamento 901 acumula o licenciamento 230 recebido pela unidade de recebimento de licenciamento 903. Neste caso, a fim de permitir que apenas o dispositivo terminal 103 utilize o licenciamento 230, é comum que o licenciamento 230 seja criptografado de acordo com uma criptografia local e então acumulado.

A unidade de gerenciamento de informação única 902 gerencia a informação única para o dispositivo terminal 103, e obtém informações únicas, como, por exemplo, uma chave secreta do dispositivo terminal 103 necessária para estabelecer um canal SAC com o servidor de licenciamento 101, e um certificado de chave pública do dispositivo terminal 103.

A unidade de recebimento de licenciamento 903 recebe o licenciamento 230 do servidor de licenciamento 101 através do canal SAC.

A unidade de gerenciamento de licenciamento 904 gerencia o licenciamento 230 acumulado na unidade de armazenamento de licenciamento 901.

A unidade de recebimento de conteúdo 905 recebe o conteúdo do servidor de conteúdo 102 através de uma rede de protocolo IP ou coisa do gênero. A unidade de recebimento de conteúdo 905 obtém os fluxos TS a partir do conteúdo recebido, e transmite os fluxos TS para a unidade de desmultiplexação 906.

A unidade de desmultiplexação 906 é uma unidade para a obtenção de um conteúdo criptografado multiplexado a partir de um padrão MPEG-2 TS, e da desmultiplexação do conteúdo da mensagem ECM 220 ou coisa do gênero. A unidade de desmultiplexação 906 obtém o vídeo e áudio do conteúdo e o PID de cada pacote de fluxo TS incluindo a mensagem ECM 220 com referência à informações PSI, tais como a tabela PAT (Program Association Table) (Tabela de Associação de Programas) e a tabela PMT (Program Map Table) (Tabela de Mapas de Programa) incluídas no fluxo TS recebido pela unidade de recebimento de conteúdo 905.

A unidade de obtenção de informação de hora 907 gerencia o

tempo corrente. Pressupõe-se que a unidade de obtenção de informação de hora 907 seja, por exemplo, um relógio capaz de gerenciar precisamente o tempo corrente dentro do dispositivo terminal 103, ou, conforme apropriado, um relógio, um cronômetro ou coisa do gênero que opera com base no tempo corrente obtido de um servidor confiável em uma rede através de uma tabela TOT (Time Offset Table) (Tabela de Desvio de Tempo) em difusão via uma passagem segura de comunicação. Além disso, uma prioridade pode ser aplicada a estas informações de tempo confiáveis na obtenção. Nesta modalidade, pressupõe-se que a unidade de obtenção de informação de hora 907 obtenha uma informação de tempo confiável de um servidor de tempo na rede através da unidade de obtenção de informação de hora não mostrada na figura 11, e obtenha o tempo com base na informação de tempo obtida.

A unidade de descriptografia de informação relacionada 908 descriptografa a mensagem ECM 220 por meio do uso de uma chave de trabalho Kw 203. Em termos mais específicos, a unidade de descriptografia de informação relacionada 908 obtém o licenciamento 230 tendo um identificador ID de chave de trabalho 402 correspondente da unidade de armazenamento de licenciamento 901 por meio da referência ao identificador ID de chave de trabalho 602 da mensagem ECM 220 obtida a partir da unidade de desmultiplexação 906, e, no caso de ter o licenciamento 230, descriptografa a mensagem ECM 220 por meio do uso da chave de trabalho Kw 203 gerada na chave de trabalho Kw 401 do licenciamento 230.

A unidade de julgamento de recepção em tempo real 909 julga se a diferença entre a data e hora de transmissão 603 gerada em uma mensagem ECM 220 e o tempo corrente obtido a partir da unidade de obtenção de informação de hora 907 se encontra abaixo de um valor predeterminado, e com base no resultado, julga se o conteúdo recebido pela unidade de recebimento de conteúdo 905 está sendo recebido em tempo real (se o conteúdo está sendo correntemente transmitido a partir do servidor de conteúdo 102).

Nos métodos gerais para o julgamento de tais períodos válidos

de acordo com os métodos convencionais de recepção limitada, a data e hora de transmissão incluídas em uma mensagem ECM são comparadas com o período válido de um contrato obtido no dispositivo terminal. No entanto, de acordo com tais métodos, é possível se usar constantemente (visualizar ou gravar) um conteúdo várias vezes no caso em que a data e hora de transmissão incluídas em uma mensagem ECM são de um valor dentro do período válido de contrato. A aplicação de tais métodos para a difusão de serviços de acordo com o esquema de protocolo IP (chamado de multidifusão de protocolo IP, difusão de protocolo IP, ou coisa do gênero) redunda no problema de que o conteúdo pode ser usado várias vezes de uma maneira não autorizada ao se obter o conteúdo através de um PC (Personal Computer) (Computador Pessoal) ou coisa do gênero de uma maneira relativamente simples, acumulando o conteúdo, e entrando o conteúdo acumulado no dispositivo terminal 103 várias vezes. Sendo assim, nesta modalidade, sabe-se se um conteúdo é recebido em tempo real ao se verificar a data e hora de transmissão 603 incluídas na mensagem ECM 220 por meio do uso do tempo corrente obtido a partir de uma fonte confiável. Isto torna possível se limitar o uso do conteúdo no momento de recepção em tempo real a apenas uma única vez, e, deste modo, impedir o uso do conteúdo acumulado no caso em que o conteúdo é entrado (re-transmitido) diversas vezes. Além disso, é realmente difícil sincronizar de maneira precisa o tempo corrente obtido pela unidade de obtenção de informação de hora 907 e a data e a hora da data e hora de transmissão 603. Sendo assim, na presente modalidade, uma faixa de erro permissível no processo de julgamento de recepção em tempo real feito pela unidade de julgamento de recepção em tempo real 909 é obtida de antemão, e quando a diferença entre o tempo corrente obtido pela unidade de obtenção de informação de hora 907 e a data e a hora da data e hora de transmissão 603 recai dentro da faixa de erro permissível, o conteúdo é julgado como sendo recebido em tempo real.

A unidade de detecção de manipulação 910 detecta a manipulação de uma mensagem ECM 220 ao fazer um julgamento de consistência se duas datas e horas de transmissão 603 e dois códigos de julgamento de

contrato 604 gerados em uma mensagem ECM 220 são respectivamente idênticos.

A unidade de julgamento de detalhes de contrato 911 pode descriptografar a mensagem ECM 220 como o resultado dos processos realizados pela unidade de descriptografia de informação relacionada 908, pela unidade de julgamento de recepção em tempo real 909, e pela unidade de detecção de manipulação 910. Além disso, no caso em que a validade da mensagem ECM 220 é verificada (em outras palavras, a mensagem ECM 220 não foi manipulada, e, portanto, válida), a unidade de julgamento de detalhes de contrato 911 faz um julgamento sobre a disponibilidade da chave de misturação Ks 201 com base no licenciamento 230 e na mensagem ECM 220 obtida a partir da unidade de gerenciamento de licenciamento 904. Além disso, quando a unidade de julgamento de detalhes de contrato 911 julga que o uso de uma chave de misturação Ks 201 é permitido, como um resultado do julgamento sobre a disponibilidade, a mesma notifica a unidade de controle de uso de conteúdo 912 ou a unidade de controle de armazenamento de conteúdo 913 do fato e transmite a chave de misturação Ks 201 para a mesma.

A unidade de controle de uso de conteúdo 912 reproduz o conteúdo recebido. Além disso, quando a unidade de controle de uso de conteúdo 912 recebe a chave de misturação Ks 201 como o resultado dos processos realizados pela unidade de descriptografia de informação relacionada 908, pela unidade de julgamento de recepção em tempo real 909, pela unidade de detecção de manipulação 910, e pela unidade de julgamento de detalhes de contrato 911, a mesma descriptografa o conteúdo recebido da unidade de recebimento de conteúdo 905 por meio do uso da chave de misturação Ks 201 obtida, e realiza um processo de reprodução. Neste momento, a unidade de controle de uso de conteúdo 912 controla a saída de reprodução digital/a saída de reprodução analógica, com base na informação de controle de saída 406 obtida a partir da unidade de gerenciamento de licenciamento 904.

A unidade de controle de armazenamento de conteúdo 913 é

uma unidade que grava o conteúdo recebido em um meio de gravação interno ou externo ou coisa do gênero. Além disso, a unidade de controle de armazenamento de conteúdo 913 pode receber a chave de misturação Ks 201 como o resultado dos processos realizados pela unidade de descriptografia de informação relacionada 908, pela unidade de julgamento de recepção em tempo real 909, pela unidade de detecção de manipulação 910, e pela unidade de julgamento de detalhes de contrato 911. Além disso, no caso em que a informação de controle de saída 406 obtida a partir da unidade de gerenciamento de licenciamento 904 permite tal gravação, a unidade de controle de armazenamento de conteúdo 913 descriptografa o conteúdo recebido da unidade de recebimento de conteúdo 905 por meio do uso da chave de misturação Ks 201 obtida, converte o conteúdo descriptografado para um formato predeterminado de acordo com o meio de gravação como o destino de gravação, e criptografa e grava o conteúdo.

Em seguida, é feita a descrição das operações do sistema de distribuição de conteúdo 1 da presente modalidade com referência ao fluxograma.

Primeiramente, com referência ao fluxograma da figura 12, é feita uma descrição de como o dispositivo terminal 103 desta modalidade recebe um licenciamento 230 do servidor de licenciamento 101.

S1001: A unidade de gerenciamento de licenciamento 904 gera uma solicitação de licenciamento pedindo o servidor de licenciamento 101 para prover o licenciamento 230, e transmite a solicitação de licenciamento para a unidade de recebimento de licenciamento 903. A unidade de recebimento de licenciamento 903 transmite a solicitação de licenciamento para o servidor de licenciamento 101 através do canal SAC.

S1002: A unidade de transmissão de licenciamento 305 recebe a solicitação de licenciamento do dispositivo terminal 103. A unidade de transmissão de licenciamento 305 transmite a solicitação de licenciamento recebida para a unidade de geração de licenciamento 304.

S1003: A unidade de geração de licenciamento 304 verifica o status de contrato do dispositivo terminal 103 autenticado através do canal

SAC por meio do uso da unidade de acumulação de informações de contrato 302, e julga a presença/ausência do contrato para o dispositivo terminal 103 (usuário β). Em termos mais específicos, primeiro, a unidade de geração de licenciamento 304 obtém informações de identificação do licenciamento solicitado através da solicitação de licenciamento recebida na etapa S1002, e verifica se a informação de contrato para o dispositivo terminal 103 está acumulada na unidade de acumulação de informações de contrato 302. No caso em que a informação de contrato é obtida na unidade de acumulação de informações de contrato 302, a unidade de geração de licenciamento 304 verifica ainda se o contrato expirou. Quando o resultado da verificação mostra que nenhuma informação de contrato está acumulada na unidade de acumulação de informações de contrato 302, ou o contrato expirou, a unidade de geração de licenciamento 304 julga se o contrato não é válido (sem contrato). Por outro lado, quando a informação de contrato é acumulada na unidade de acumulação de informações de contrato 302, e o contrato não expirou, a unidade de geração de licenciamento 304 julga se o contrato é válido (existe um contrato). Quando o julgamento é "existe um contrato" neste processo, é feita uma transição para o processo da etapa S1004. Quando o julgamento é "sem contrato" neste processo, é feita uma transição para o processo da etapa S1005.

S1004: A unidade de geração de licenciamento 304 gera o licenciamento 230 mostrado na figura 5. A unidade de geração de licenciamento 304 obtém, da unidade de acumulação de chaves de trabalho 301, a chave de trabalho Kw 401 e o identificador ID de chave de trabalho 402 da figura 5, e gera os mesmos no licenciamento 230. Além disso, a unidade de geração de licenciamento 304 obtém, da unidade de acumulação de informações de contrato 302, informações relativas ao contrato de serviço feito para o dispositivo terminal 103 (usuário β), e gera o código de contrato 403, a data e hora de partida 404, a data e hora de finalização 405, e a informação de controle de saída 406. A unidade de geração de licenciamento 304 transmite o licenciamento 230 gerado para a unidade de transmissão de licenciamento 305.

S1005: A unidade de transmissão de licenciamento 305 gera uma resposta à solicitação de licenciamento, e transmite a resposta para o dispositivo terminal 103. A unidade de transmissão de licenciamento 305 gera uma resposta à solicitação de licenciamento incluindo o licenciamento 230 no caso em que a unidade de geração de licenciamento 304 gera o licenciamento 230 na etapa S1004. Paralelamente, no caso em que a unidade de geração de licenciamento 304 não gera o licenciamento 230 na etapa S1004, a unidade de transmissão de licenciamento 305 gera a resposta à solicitação de licenciamento não incluindo o licenciamento 230, porém incluindo a informação que notifica que o licenciamento 230 não pode ser transmitido.

S1006: A unidade de recebimento de licenciamento 903 recebe a resposta à solicitação de licenciamento do servidor de licenciamento 101.

S1007: A unidade de gerenciamento de licenciamento 904 verifica se o licenciamento 230 foi recebido, referindo-se à resposta à solicitação de obtenção de licenciamento. No caso em que o licenciamento 230 é recebido, é feita uma transição para o processo da etapa S1008. No caso em que o licenciamento 230 não é recebido, o processamento é finalizado.

S1008: A unidade de gerenciamento de licenciamento 904 armazena o licenciamento 230 recebido na etapa S1007 na unidade de armazenamento de licenciamento 901.

Foi feita na modalidade acima uma descrição das operações de uma transmissão e recepção de um licenciamento.

Em seguida, com referência ao fluxograma da figura 13, é feita uma descrição de como o servidor de conteúdo 102 realiza uma operação de transmissão de conteúdo para o dispositivo terminal 103.

S1101: A unidade de codificação de conteúdo 504 julga se o conteúdo está sendo transmitido de acordo com uma instrução por um sistema de fluxo ascendente (por exemplo, um sistema de gerenciamento de operação de programa) ou coisa do gênero. Em termos mais específicos, a unidade de codificação de conteúdo 504 segue para o processo da etapa S1102 quando a unidade de codificação de conteúdo 504 não recebe do

sistema de fluxo ascendente ou coisa do gênero nenhuma instrução para cancelar a codificação ou a transmissão do conteúdo. Quando a unidade de codificação de conteúdo 504 recebe do sistema de fluxo ascendente ou coisa do gênero uma instrução para cancelar a codificação ou transmissão do conteúdo, o processamento finaliza.

S1102: A unidade de codificação de conteúdo 504 lê a partir da unidade de acumulação de conteúdo 501 o conteúdo especificado pelo sistema de fluxo ascendente ou coisa do gênero, codifica o conteúdo de acordo com o padrão MPEG-2, H. 264, ou coisa do gênero a fim de gerar fluxos TS incluindo o conteúdo. A unidade de codificação de conteúdo 504 em seguida transmite os fluxos TS gerados para a unidade de criptografia de conteúdo 506.

S1103: A unidade de geração de misturação de chaves 505 gera chaves de misturação Ks 201 com base em números aleatórios de acordo com seus períodos de atualização, e transmite é mesmas para a unidade de criptografia de conteúdo 506 e para a unidade de geração de informação relacionada 508.

S1104: A unidade de criptografia de conteúdo 506 em seguida codifica é cargas úteis dos respectivos pacotes de fluxo TS do conteúdo recebido a partir da unidade de codificação de conteúdo 1102 por meio do uso das chaves de misturação Ks 201 recebidas da unidade de geração de misturação de chaves 505. Deve-se notar que a unidade de criptografia de conteúdo 506 comuta é chaves de misturação Ks 201 de modo a criptografar os pacotes de fluxo TS de acordo com os períodos de atualização das chaves de misturação Ks 201, e ao mesmo tempo, atualiza os valores de transport_scrambling_control das porções de cabeçalho dos respectivos pacotes de fluxo TS de acordo com o par/ímpar. A unidade de criptografia de conteúdo 506 transmite os fluxos TS criptografados para a unidade de multiplexação 510.

S1105: A unidade de geração de informação relacionada 508 gera a mensagem ECM 220 mostrada na figura 7 no momento da transmissão do conteúdo. Em termos mais específicos, a unidade de geração de in-

formação relacionada 508 obtém da unidade de acumulação de chaves de trabalho 503 o identificador ID de chave de trabalho 602 da chave de trabalho Kw 203 a ser aplicada, e gera o mesmo na mensagem ECM 220. Em seguida, a unidade de geração de informação relacionada 508 obtém o tempo corrente da unidade de identificação de data e hora de transmissão 507, e gera o tempo corrente nas duas datas e horas de transmissão 603. Em seguida, a unidade de geração de informação relacionada 508 obtém informações de atributo do conteúdo da unidade de acumulação de informações de atributos de conteúdo 502, gera um código de julgamento de contrato 604 de modo a julgar se o conteúdo pode ser usado no dispositivo terminal 103, e gera o mesmo na mensagem ECM 220 como os dois códigos de julgamento de contrato 604. Além disso, conforme mostrado na figura 8, a unidade de geração de informação relacionada 508 insere dados privativos 605 na mensagem ECM 220 a fim de gerar a chave de misturação (ímpar) 606 e a chave de misturação (par) 607 de tal maneira que a chave de misturação (ímpar) 606 e a chave de misturação (par) 607 fiquem alinhadas ao bloco de criptografia que sucede o bloco de criptografia incluindo a data e hora de transmissão 603 e o código de julgamento de contrato 604. Por último, a unidade de geração de informação relacionada 508 obtém a chave de misturação (ímpar) 606 e a chave de misturação (par) 607 da unidade de geração de misturação de chaves 505, e gera é mesmas na mensagem ECM 220. A unidade de geração de informação relacionada 508 transmite a mensagem ECM gerada 220 para a unidade de criptografia de informação relacionada 509.

S1106: A unidade de criptografia de informação relacionada 509 obtém a chave de trabalho Kw 203 correspondente a partir da unidade de acumulação de chaves de trabalho 503 por meio da referência ao identificador ID de chave de trabalho 602 da mensagem ECM 220 recebida da unidade de geração de informação relacionada 508, e criptografa é porções de criptografia da mensagem ECM 220 no modo CBM. A unidade de criptografia de informação relacionada 509 converte a mensagem ECM criptografada 220 em pacotes de fluxo TS, e em seguida transmite os mesmos para a uni-

dade de multiplexação 510.

S1107: A unidade de multiplexação 510 multiplexa os fluxos TS do conteúdo recebido criptografado e a mensagem ECM 220, e em seguida transmite os mesmos para a unidade de transmissão 511.

S1108: A unidade de transmissão 511 transmite os fluxos TS recebidos da unidade de multiplexação 510 para o dispositivo terminal 103, e em seguida continua para o processo da etapa S1101.

Na presente modalidade, foi feita acima a descrição de operações do processo de transmissão de conteúdo.

Em seguida, com referência ao fluxograma da figura 14, é feita a descrição de como o dispositivo terminal 103 nesta modalidade recebe o conteúdo transmitido a partir do servidor de conteúdo 102.

S1201: A unidade de recebimento de conteúdo 905 recebe o conteúdo transmitido a partir do servidor de conteúdo 102. O conteúdo recebido é convertido em fluxos TS, e os fluxos TS são em seguida transmitidos para a unidade de desmultiplexação 906.

S1202: A unidade de recebimento de conteúdo 905 verifica se o conteúdo a partir do servidor de conteúdo 102 está sendo recebido. Quando o conteúdo está sendo recebido, é feita uma transição para o processo da etapa S1203. Por outro lado, quando o conteúdo não está sendo recebido, o processamento é finalizado.

S1203: A unidade de desmultiplexação 906 desmultiplexa os fluxos TS recebidos da unidade de recebimento de conteúdo 905 em uma mensagem ECM 220 e em pacotes de fluxo TS. A unidade de desmultiplexação 906 transmite o conteúdo desmultiplexado para a unidade de controle de uso de conteúdo 912 ou para a unidade de controle de armazenamento de conteúdo 913, e transmite a mensagem ECM desmultiplexada 220 para a unidade de descriptografia de informação relacionada 908.

S1204: A unidade de descriptografia de informação relacionada 908 verifica se o licenciamento 230 incluindo a chave de trabalho Kw 203 da unidade de gerenciamento de licenciamento 904 é obtido por meio da referência ao identificador ID de chave de trabalho 602 da mensagem ECM 220

recebida da unidade de desmultiplexação 906. Em termos mais específicos, a unidade de descriptografia de informação relacionada 908 transmite o identificador ID de chave de trabalho 602 para a unidade de gerenciamento de licenciamento 904. Em seguida, a unidade de gerenciamento de licenciamento 904 pesquisa a unidade de armazenamento de licenciamento 901 para o licenciamento 230 com o ID de chave de trabalho 402 idêntico ao ID de chave de trabalho 602 recebido.

No caso em que a chave de trabalho Kw 203 correspondente ao identificador ID de chave de trabalho 602 é obtida, é feita a transição para a etapa S1205. Por outro lado, no caso em que a chave de trabalho Kw 203 correspondente ao identificador ID de chave de trabalho 602 não é obtida, o processamento finaliza.

S1205: A unidade de descriptografia de informação relacionada 908 descriptografa é porções de criptografia da mensagem ECM 220 por meio do uso da chave de trabalho Kw 203 obtida da unidade de gerenciamento de licenciamento 904. A unidade de descriptografia de informação relacionada 908 transmite a mensagem ECM descriptografada 220 para a unidade de julgamento de recepção em tempo real 909.

S1206: A unidade de julgamento de recepção em tempo real 909, a unidade de detecção de manipulação 910, e a unidade de julgamento de detalhes de contrato 911 realizam o processo de julgamento de mensagem ECM a ser descrito mais adiante com referência à figura 15.

S1207: A unidade de julgamento de detalhes de contrato 911 julga se a chave de misturação Ks 201 pode ser obtida. No caso em que a chave de misturação Ks 201 é obtida, é feita uma transição para o processo da etapa S1208. No caso em que a chave de misturação Ks 201 não é obtida, o processamento finaliza.

S1208: A unidade de controle de uso de conteúdo 912 ou a unidade de controle de armazenamento de conteúdo 913 descriptografa os pacotes de fluxo TS do conteúdo criptografado em seguida recebido da unidade de desmultiplexação 906 por meio do uso da chave de misturação Ks 201 recebida a partir da unidade de julgamento de detalhes de contrato 911.

S1209: A unidade de controle de uso de conteúdo 912 usa o conteúdo com base na informação de controle de saída 615 extraída da mensagem ECM 230 e/ou da informação de controle de saída 406 recebida da unidade de gerenciamento de licenciamento 904. A unidade de controle de uso de conteúdo 912 verifica a informação de controle de saída 615 e/ou a informação de controle de saída 406, e emite o conteúdo para uma saída digital/saída analógica de acordo com é especificações da informação de controle de saída 615 e/ou da informação de controle de saída 406. Além disso, a unidade de controle de armazenamento de conteúdo 913 verifica a informação de controle de saída 615 e/ou a informação de controle de saída 406, e no caso em que o conteúdo pode ser gravado (por exemplo, a informação CCI é uma Cópia Livre), a mesma realiza os processos de conversão e criptografia do conteúdo em um formato predeterminado em conformidade com o meio de gravação como um destino de gravação, e grava o conteúdo. Nota-se que, no caso em que o conteúdo não pode ser gravado (por exemplo, a informação CCI é Nunca Copie), o processamento finaliza sem gravar o conteúdo.

Deve-se notar que, no caso em que a mensagem ECM criptografada 220 foi manipulada, mas se julga que nenhuma manipulação foi feita na mensagem ECM 220 do processo de julgamento de mensagem ECM da etapa S1205, a decodificação do conteúdo falhará nesta etapa, uma vez que a chave de misturação K (ímpar) 606 e chave de misturação Ks (par) 607 descriptografadas não têm os corretos valores.

Foi feita acima a descrição das operações do processo de recepção de conteúdo na presente modalidade.

Em seguida, com referência ao fluxograma mostrado na figura 15, é feita uma descrição de como o dispositivo terminal 103 realiza operações do processo de julgamento de mensagem ECM de modo a julgar a disponibilidade da mensagem ECM 220. Deve-se notar que este processo de julgamento de mensagem ECM mostra detalhes da etapa S1206 da figura 14.

S1301: A unidade de julgamento de recepção em tempo real

909 realiza um processo de julgamento de recepção em tempo real a ser descrito mais adiante com referência à figura 16.

S1302: A unidade de julgamento de recepção em tempo real 909 verifica se o conteúdo e a mensagem ECM 220 estão sendo recebidas "em tempo real" através do processo da etapa S1301. Quando se julga que o conteúdo e a mensagem ECM 220 estão sendo recebidos "em tempo real", é feita uma transição para o processo da etapa S1303. Por outro lado, quando se julga que o conteúdo e a mensagem ECM 220 são recebidas "não em tempo real" (por exemplo, o conteúdo e a mensagem ECM 220 são acumuladas e em seguida re-transmitidas), o processamento finaliza.

S1303: A unidade de detecção de manipulação 910 realiza um processo de detecção de manipulação a ser descrito mais adiante com referência à figura 17.

S1304: No caso em que a unidade de detecção de manipulação 910 faz um julgamento, no processo da etapa S1303, que não foi feita "nenhuma manipulação" na mensagem ECM 220, é feita a transição para a etapa S1305. Por outro lado, no caso em que a unidade de detecção de manipulação 910 faz o julgamento de que "a mensagem ECM foi manipulada", o processamento finaliza.

S1305: A unidade de julgamento de detalhes de contrato 911 realiza um processo de julgamento de detalhes de contrato a ser descrito mais adiante com referência à figura 18.

S1306: Quando se julga que "existe um contrato" como o resultado do processamento da etapa S1305, a unidade de julgamento de detalhes de contrato 911 realiza o processo da etapa S1307. Por outro lado, quando é julgado como "sem contrato", o processamento finaliza.

S1307: A unidade de julgamento de detalhes de contrato 911 obtém a chave de misturação Ks (ímpar) e a chave de misturação Ks (par) 607 a partir da mensagem ECM 220.

Em seguida, com referência ao fluxograma da figura 16, é feita uma descrição das operações do processo de julgamento de recepção em tempo real da etapa S1301 da figura 15.

S1401: A unidade de julgamento de recepção em tempo real 909 obtém o tempo corrente da unidade de obtenção de informação de hora 907.

S1402: A unidade de julgamento de recepção em tempo real 909 calcula a diferença entre é datas e horas de transmissão 603 da mensagem ECM 220 e o tempo corrente obtido da unidade de obtenção de informação de hora 907. Em termos mais específicos, a unidade de julgamento de recepção em tempo real 909 lê pelo menos uma data e hora de transmissão 603 dentre é datas e horas de transmissão 603 incluídas em uma mensagem ECM 220. Em seguida, a unidade de julgamento de recepção em tempo real 909 compara o valor da data e hora de transmissão 603 e o valor do tempo corrente obtido a partir da unidade de obtenção de informação de hora 907. Quando o valor da data e hora de transmissão 603 é maior, a unidade de julgamento de recepção em tempo real 909 subtrai o valor de data e hora de transmissão 603 do valor do tempo corrente de modo a obter um valor desejado.

S1403: A unidade de julgamento de recepção em tempo real 909 julga se o valor de diferença calculado na etapa S1402 é igual ou menor que o valor definido anteriormente obtido. Quando a valor de diferença é igual ao ou menor que o valor definido, é feita uma transição para o processo da etapa S1404. Quando a valor de diferença é maior que o valor definido, é feita uma transição para o processo da etapa S1405.

S1404: A unidade de julgamento de recepção em tempo real 909 julga se o conteúdo e a mensagem ECM 220 estão sendo recebidos "em tempo real".

S1405: A unidade de julgamento de recepção em tempo real 909 julga se o conteúdo e a mensagem ECM 220 estão sendo recebidos "não em tempo real".

Foi feita acima a descrição das operações do processo de julgamento de recepção em tempo real na presente modalidade.

Em seguida, com referência ao fluxograma da figura 17, é feita a descrição das operações do processo de detecção de manipulação da etapa

S1303 da figura 15.

S1501: A unidade de detecção de manipulação 910 julga se é duas datas e horas de transmissão 603 incluídas na mensagem ECM 220 são idênticas. Quando é mesmas são idênticas, é feita uma transição para o processo da etapa S1502. Por outro lado, quando é mesmas não são idênticas, é feita uma transição para o processo da etapa S1504.

S1502: A unidade de detecção de manipulação 910 julga se os dois códigos de julgamento de contrato 604 incluídos na mensagem ECM 220 são idênticos. Quando os mesmos são idênticos, é feita uma transição para o processo da etapa S1503. Por outro lado, quando os mesmos não são idênticos, é feita uma transição para o processo da etapa S1504.

S1503: A unidade de detecção de manipulação 910 julga se não foi feita "nenhuma manipulação" na mensagem ECM 220.

S1504: A unidade de detecção de manipulação 910 julga se "a mensagem ECM 220 foi manipulada".

Foi feita acima uma descrição das operações do processo de detecção de manipulação na presente modalidade.

Em seguida, com referência ao fluxograma da figura 18, é feita uma descrição das operações do processo de julgamento de detalhes de contrato da etapa S1305 da figura 15.

S1601: A unidade de julgamento de detalhes de contrato 911 lê o licenciamento 230 correspondente ao conteúdo da unidade de gerenciamento de licenciamento 904. Em termos mais específicos, a unidade de julgamento de detalhes de contrato 911 solicita à unidade de gerenciamento de licenciamento 904 para transmitir o licenciamento 230 incluindo a chave de trabalho Kw 203 correspondente ao identificador ID de chave de trabalho 602. A unidade de gerenciamento de licenciamento 904 pesquisa a unidade de armazenamento de licenciamento 901 para o licenciamento 230, e transmite o licenciamento 230 para a unidade de julgamento de detalhes de contrato 911.

S1602: A unidade de julgamento de detalhes de contrato 911 compara a data e hora de transmissão 603 da mensagem ECM 220 e a data

e hora de partida 404 e a data e hora de finalização 405 do licenciamento 230. No caso em que a data e hora de transmissão 603 está entre a data e hora de partida 404 e a data e hora de finalização 405, o processamento da etapa S1603 é executado. No caso em que a data e hora de transmissão 603 não está entre a data e hora de partida 404 e a data e hora de finalização 405, o processamento da etapa S1606 é executado. Deve-se notar que, no caso em que uma dentre a data e hora de partida 404 e a data e hora de finalização 405 não especifica nenhum período válido (nenhuma definição para o período válido), é desnecessário se comparar o valor da data e hora de transmissão 603 ou ainda da data e hora de partida 404 ou da data e hora de finalização 405, e pressupõe-se que a data e hora de transmissão 603 está entre a data e hora de partida 404 e a data e hora de finalização 405.

S1603: A unidade de julgamento de detalhes de contrato 911 calcula o valor AND (produto lógico) do código de contrato 403 do licenciamento 230 e do código de julgamento de contrato 604 da mensagem ECM 220.

S1604: A unidade de julgamento de detalhes de contrato 911 faz um julgamento se o resultado do processo da etapa S1603 é "não zero". S1603: Quando o resultado do processo da etapa S1603 é "não zero", é feita uma transição para o processo da etapa S1605. Por outro lado, quando o resultado é "não zero", é feita uma transição para o processo da etapa S1606.

S1605: A unidade de julgamento de detalhes de contrato 911 julga se "existe um contrato".

S1606: A unidade de julgamento de detalhes de contrato 911 julga como "sem contrato".

Foi feita acima a descrição das operações do processo de julgamento de detalhes de contrato na presente modalidade.

O licenciamento 230 distribuído pelo servidor de licenciamento 101 é distribuído através do canal SAC na presente modalidade. No entanto, deve-se notar que o servidor de licenciamento 101 pode ser distribuído na forma de dados que forma criptografados e submetidos à detecção de mani-

pulação de modo a permitir que apenas o dispositivo terminal 103 do usuário β descriptografe e obtenha o licenciamento 230. Este formato de dado é chamado EMM (Entitlement Management Message) (Mensagem de Gerenciamento de Titularidade). Além disso, os dados tendo um formato de dado do licenciamento 230 são distribuídos nesta modalidade, mas os formatos de dado não se limitam a este aspecto, contanto que itens de dados conforme incluídos no licenciamento 230 possam ser distribuídos a partir do servidor de licenciamento 101 para o dispositivo terminal 103.

Além disso, nesta modalidade, é bom fazer com que módulos à prova de violação executem o gerenciamento das e o processamento feito nas informações para é quais a segurança vem a ser um requisito especial. Exemplos de tais módulos à prova de violação incluem um cartão IC ou um LSI de segurança, e tais gerenciamento e processamento são feitos por uma unidade de obtenção de informação de hora 907, uma unidade de descriptografia de informação relacionada 908, uma unidade de julgamento de tempo de transmissão 909, uma unidade de detecção de manipulação 910, e uma unidade de julgamento de detalhes de contrato 911 do dispositivo terminal 103.

Além disso, o compartilhamento de funções do sistema servidor (o servidor de licenciamento 101, o servidor de conteúdo 102) do provedor α não se limita à configuração mostrada na presente modalidade, e algumas funções podem estar incluídas em um servidor que não seja os servidores da presente modalidade, e podem ser implementadas em servidores que não estejam fisicamente emparelhados.

Além disso, o código de contrato 403 (bits de nível) é usado como uma informação que mostra o contrato do usuário β na presente modalidade, porém a presente invenção não se limita a este aspecto. Com efeito, a presente invenção é aplicável mesmo que seja feito um julgamento dos detalhes do contrato por meio do uso de um identificador tal como um identificador ID de contrato.

Além disso, embora seja considerado um caso exemplar no qual pacotes de fluxo TS criptografados por uma unidade de criptografia de con-

teúdo 506 são multiplexados por uma unidade de multiplexação 510 com relação à criptografia de conteúdo no servidor de conteúdo 102, o conteúdo pode ser criptografado por uma unidade de criptografia de conteúdo 506 através da multiplexação por uma unidade de multiplexação 510.

Além disso, embora um caso exemplar seja considerado, no qual o servidor de conteúdo 102 na presente modalidade lê o conteúdo acumulado no conteúdo DB 305, e a unidade de codificação de conteúdo 504 codifica o mesmo em tempo real, será conveniente que os fluxos TS sejam gerados off-line anteriormente e acumulados na unidade de acumulação de conteúdo 501, e, dessa forma, omitir o processo de codificação da unidade de codificação de conteúdo 504 no momento de transmissão de conteúdo.

Além disso, embora um caso exemplar seja considerado, no qual o servidor de conteúdo 102 na presente modalidade gera o conteúdo a ser transmitido a partir da unidade de acumulação de conteúdo 501, será conveniente que uma fonte, tal como uma difusão ao vivo, seja diretamente entrada para a unidade de codificação de conteúdo 504 sem usar a unidade de acumulação de conteúdo 501.

Além disso,embora o servidor de conteúdo 102 na presente modalidade seja concebido para seqüencialmente gerar chaves de misturação Ks 201 na unidade de geração de misturação de chaves 505, é conveniente que é chaves de misturação Ks 201 sejam geradas anteriormente e é acumuladas sejam aplicadas.

Quanto a disposição de dados das porções de criptografia da mensagem ECM 220 na presente modalidade, conforme mostrado na figura 8, um caso exemplar é considerado no qual a chave de misturação KS (ímpar) 606 e a chave de misturação Ks (par) 607 são alinhadas em blocos de criptografia que sucedem o bloco de criptografia da data e hora de transmissão 603 e o código de julgamento de contrato 604. No entanto, como no caso da presente modalidade, um efeito de prevenção de manipulação pode ser obtido mesmo quando a chave de misturação Ks (ímpar) 606 ou a chave de misturação Ks (par) 607 que sucedem a data e hora de transmissão 603 e o código de julgamento de contrato 604 são dispostas, em alinhamento

uma à outra, em dois blocos de criptografia consecutivos, e a chave de misturação Ks (ímpar) 606 e a chave de misturação Ks (par) 607 são dispostas através de dois blocos de criptografia consecutivos.

Além disso, embora a informação de controle de saída 406 seja incluída no licenciamento 230 na presente modalidade, é conveniente que a informação de controle de saída 406 seja incluída na mensagem ECM 220. Neste caso, por exemplo, um método concebível é a geração da informação de controle de saída 406 nas posições dos dois dados privativos 605 da mensagem ECM 220, a realização de uma verificação de consistência das duas informações de controle de saída 406 depois da descriptografia da mensagem ECM 220 no dispositivo terminal 103, e a realização da detecção de manipulação na informação de controle de saída 406.

Na presente modalidade, um caso exemplar é considerado, no qual a unidade de julgamento de recepção em tempo real 909 obtém anteriormente um valor predefinido da diferença de comparação em tempo entre a data e hora de transmissão 603 da mensagem ECM 220 e o tempo corrente na unidade de obtenção de informação de hora 907. No entanto, é vantajoso que este valor predefinido seja dinamicamente alterável a partir de uma base de provedor para uma base de contrato ou conteúdo. Neste caso, é conveniente que a informação de controle de saída 406 seja distribuída juntamente com o licenciamento 230 e com a informação de tempo confiável através do canal SAC ou distribuída na mensagem ECM 220. Quando incluído na mensagem ECM 220, por exemplo, um método concebível é a geração da informação de controle de saída 406 nas posições dos dois dados privativos 605 da mensagem ECM 220, a realização de uma verificação de consistência das duas informações de controle de saída 406 após a descriptografia da mensagem ECM 220 no dispositivo terminal 103, e a realização da detecção de manipulação na informação de controle de saída 406. Além disso, é conveniente se realizar o processo de julgamento de recepção em tempo real de acordo com os detalhes da informação de controle de saída 406. Por exemplo, é concebível que este processamento não seja executado no caso em que a informação CCI da informação de controle de saída é uma Cópia Li-

vre, ou mostra que a gravação não é permitida.

Além disso, embora o dispositivo terminal 103 seja configurado para acumular é chaves de trabalho Kw 203 (licenciamentos 230) na unidade de armazenamento de licenciamento 901 na presente modalidade, será vantajoso, porém, que é chaves de trabalho K2 203 sejam obtidas a partir do servidor de licenciamento 101 conforme necessário e guardadas.

Além disso, quanto ao processamento realizado pelo dispositivo terminal 103 na presente modalidade, a ordem dos processos realizados pela unidade de julgamento de recepção em tempo real 909, pela unidade de detecção de manipulação 910, e pela unidade de julgamento de detalhes de contrato 911 não se limita à ordem de processamento mostrada na presente modalidade, sendo conveniente que a ordem de processamento seja alterada conforme necessário.

Além disso, no julgamento da recepção em tempo real na presente modalidade, é vantajoso se atribuir um período válido para a mensagem ECM 220, e quando o tempo corrente gerenciado por uma unidade de obtenção de informação de hora 907 estiver após o período válido, julgar como "recepção em tempo não real".

Foi descrito que o dispositivo terminal 103 não pode obter a chave de misturação Ks (ímpar) 606 e a chave de misturação Ks (par) 607 no caso em que um julgamento na etapa S1302 da figura 15 na presente modalidade seja "recepção em tempo não real"; um julgamento na etapa S1304 mostra "mensagem ECM manipulada"; e um julgamento na etapa S1306 mostra "sem contrato". No entanto, a presente invenção não se limita a estes aspectos. É conveniente que o dispositivo terminal 103 possa com sucesso obter a chave de misturação Ks (ímpar) 606 e a chave de misturação Ks (par) 607, e em seguida realize um processo de erro, conforme descrito a seguir.

(1) Proibir apenas é operações específicas. Por exemplo, a reprodução é permitida, mas a gravação não é permitida. Isto possibilita que o usuário β visualize o conteúdo mesmo quando a data e hora de transmissão 603 não está correta devido a um erro do provedor α.

(2) Exibir uma mensagem de alerta predeterminada indicando que um conteúdo anormal foi recebido e sugerir notificação a um centro de cliente (por exemplo, "Conteúdo anormal recebido. Notificar a XXX"). Deste modo, o provedor α poderá entender que um conteúdo anormal está sendo transmitido por meio da prevenção do uso não autorizado de um conteúdo e mensagem a partir de um usuário autenticado através de um telefone ou coisa do gênero.

(3) Notificar o provedor α dos detalhes do erro (tal como a ocorrência de uma recepção em tempo não real e a manipulação de uma mensagem ECM) e os detalhes da mensagem ECM incluindo tal erro (será vantajoso que a permissão do usuário seja necessária naquele momento). Isto permite a prevenção de um uso não autorizado e permite que o provedor entenda que um conteúdo anormal está sendo transmitido.

Deve-se notar que a presente invenção foi descrita com base em modalidades, porém, a presente invenção realmente não se limita às modalidades acima descritas. Os seguintes casos encontram-se também incluídos na presente invenção.

(1) Cada um dos dispositivos acima descritos configura um sistema de computador incluindo, por exemplo, um microprocessor, uma memória ROM, uma memória RAM, uma unidade de disco rígido, uma unidade de vídeo, teclados, e um mouse. Um programa de computador é gravado na memória RAM ou na unidade de disco rígido. Os respectivos dispositivos realizam suas funções por meio das quais o microprocessor operará de acordo com o programa de computador. Neste caso, a fim de realizar estas funções predeterminadas, o programa de computador é configurado pela combinação de vários códigos de instrução que indicam diretiva ao computador.

(2) Alguns ou todos os elementos estruturais que configuram os respectivos dispositivos podem ser integrados em um único sistema LSI (Large Scale Integration) (Integração de Larga Escala). O sistema de integração LSI é uma integração LSI super multifuncional fabricada por meio da integração de diversas unidades estruturais em um único chip, e, em termos

mais específicos, é um sistema de computador configurado para incluir um microprocessor, uma memória RAM, uma memória ROM, ou coisa do gênero. O programa de computador é armazenado na memória RAM. O sistema de integração LSI realiza suas funções por meio das quais o microprocessor operará de acordo com o programa de computador.

Alguns ou todos os elementos estruturais que configuram os respectivos dispositivos podem ser configurados como cartões IC anexáveis/destacáveis nos/dos respectivos dispositivos ou como módulos independentes. Desde que os cartões IC ou módulos configurem um sistema de computador incluindo um microprocessor, uma memória ROM, uma memória RAM, ou coisa do gênero, os cartões IC ou módulos poderão incluir uma integração LSI super multifuncional LSI. Estes cartões IC ou módulos realizam suas funções por meio das quais o microprocessor operará de acordo com um programa de computador. Estes cartões IC ou módulos podem ser à prova de violação.

(4) A presente invenção pode ser um método conforme mostrado acima. Além disso, a presente invenção pode ser um programa de computador para a realização de um método por meio do uso de um computador, ou pode ser um sinal digital feito no programa de computador.

Além disso, a presente invenção é um meio de gravação legível em computador no qual um programa de computador ou sinal digital é gravado. Exemplos de meios de gravação incluem um disco flexível, um disco rígido, um CD-ROM, um MO, um DVD, um DVD-ROM, um DVD-RAM, um BD (Blue-ray Disc), ou uma memória semicondutora. Além disso, a presente invenção pode ser um sinal digital gravado nestes meios de gravação.

Além disso, a presente invenção pode ser usada para a transmissão do programa de computador ou do sinal digital através de um circuito de comunicação elétrico, um circuito de comunicação sem fio ou com fio, uma rede representada pela Internet, por uma difusão de dados ou coisa do gênero.

Além disso, a presente invenção pode ser um sistema de computador incluindo um microprocessor e uma memória, cuja memória arma-

zena o programa de computador, e o microprocessor opera de acordo com o programa de computador.

Além disso, a presente invenção pode permitir que um sistema de computador independente execute o programa ou o sinal digital por meio da gravação dos mesmos no meio de gravação e transmita os mesmos via a rede ou coisa do gênero.

(5) É vantajoso se combinar de muitas maneiras a modalidade acima descrita e seus exemplos de variação.

Aplicabilidade Industrial

O sistema de distribuição de conteúdo e método de acordo com a presente invenção são úteis em um sistema para a provisão de um serviço de distribuição de conteúdo por meio do uso de uma difusão digital, um CATV, a Internet ou coisa do gênero, com servidores, dispositivos terminais, ou coisa do gênero incluídos no mesmo.

REIVINDICAÇÕES

1. Dispositivo terminal em um sistema de distribuição de conteúdo incluindo um dispositivo servidor e o dito dispositivo terminal, o dito dispositivo terminal compreendendo:

- uma unidade de recebimento configurada para receber,do dito dispositivo servidor,

(I) um conteúdo criptografado, e

(II) informações relativas a conteúdo incluindo (II-i) informações de data e hora de transmissão e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de obtenção de informação de hora configurada para obter informação de data e hora correntes, indicando uma data e hora correntes;

- uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e pela informação de tempo e uma hora indicada pelas informações de data e hora de transmissão recai dentro de uma faixa predeterminada, e julgar se o conteúdo está sendo recebido em tempo real quando a diferença de tempo recai dentro da faixa predeterminada; e

- a unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a dita unidade de julgamento de recepção em tempo real julga que o conteúdo está sendo recebido em tempo não real.

2. Dispositivo terminal, de acordo com a reivindicação 1, no qual:

- a informação relativa a conteúdo inclui uma informação de controle de saída de modo a controlar a cópia do conteúdo, e

- a dita unidade de julgamento de recepção em tempo real é configurada de modo a fazer o julgamento de acordo com os detalhes da informação de controle de saída ou omitir a realização do julgamento.

3. Dispositivo terminal, de acordo com a reivindicação 1, no qual:

- a informação de controle de saída inclui pelo menos "Cópia Livre" como uma informação para controlar a cópia do conteúdo, e

- a dita unidade de julgamento de recepção em tempo real é configurada para omitir a realização do julgamento quando a informação de controle de saída é "Cópia Livre".

4. Dispositivo terminal, de acordo com a reivindicação 1, no qual:

- a informação relativa a conteúdo inclui uma pluralidade de conjuntos de informação, cada qual incluindo um correspondente dentre é chaves de descriptografia de conteúdo e informações de data e hora de transmissão, a informação relativa a conteúdo sendo criptografada em um modo de Encadeamento de Blocos Cifrados (CBC),

- a informação relativa a conteúdo inclui uma pluralidade de chaves de descriptografia de conteúdo, e cada uma das informações de data e hora de transmissão que indica uma data e hora é disposta em um bloco de criptografia imediatamente precedente a um bloco de criptografia para uma correspondente dentre uma pluralidade de chaves de descriptografia de conteúdo,

- o dito dispositivo terminal compreende ainda uma unidade de detecção de manipulação configurada para verificar se a informação relativa a conteúdo foi manipulada ou não,

- a dita unidade de detecção de manipulação é configurada para verificar se todas as informações de data e hora de transmissão da informação relativa a conteúdo descriptografada são idênticas, e julgar se a informação relativa a conteúdo foi manipulada quando todas as informações de data e hora de transmissão não são idênticas, e

- a dita unidade de controle de uso de conteúdo é configurada ainda para limitar o uso de um conteúdo criptografado correspondente à informação relativa a conteúdo julgada como manipulada pela dita unidade de detecção de manipulação.

5. Dispositivo servidor em um sistema de distribuição de conteúdo incluindo o dito dispositivo servidor e um dispositivo terminal, o dito dis-

positivo servidor compreendendo:

- uma unidade de transmissão configurada para transmitir um conteúdo criptografado e informação relativa a conteúdo incluindo informações de data e hora de transmissão do conteúdo criptografado e uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de geração de informação relacionada configurada para gerar, na informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de identificação de data e hora de transmissão configurada para gerar, na informação relativa a conteúdo, informações de data e hora de transmissão, cada qual indicando uma data e hora na qual a informação relativa a conteúdo é transmitida; e

- uma unidade de criptografia de informação relacionada configurada para criptografar, em um modo de Encadeamento de Blocos Cifrados (CBC), a informação relativa a conteúdo na qual a pluralidade de chaves de descriptografia de conteúdo e informações de data e hora de transmissão foram geradas,

- em que a dita unidade de geração de informação relacionada é configurada para gerar, na informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo, e

- a dita unidade de identificação de data e hora de transmissão é configurada para gerar informações de data e hora de transmissão, cada qual indicando a mesma data e hora em um bloco de criptografia imediatamente precedente a um bloco de criptografia para uma correspondente dentre a pluralidade de chaves de descriptografia de conteúdo.

6. Dispositivo de geração de informação relativa a conteúdo que gera a informação relativa a conteúdo a ser transmitida juntamente com um conteúdo criptografado, o dito dispositivo de geração de informação relativa a conteúdo compreendendo:

- uma unidade de geração de informação relacionada configurada para gerar, em uma informação relativa a conteúdo, uma pluralidade de

chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de definição de data e hora de transmissão configurada para gerar, em uma informação relativa a conteúdo, informações de data e hora de transmissão, cada qual indicando uma data e hora na qual a informação relativa a conteúdo é transmitida; e

- uma unidade de criptografia de informação relacionada configurada para criptografar, em um modo de Encadeamento de Blocos Cifrados (CBC), a informação relativa a conteúdo na qual a pluralidade de chaves de descriptografia de conteúdo e informações de data e hora de transmissão foram geradas,

- em que a dita unidade de geração de informação relacionada é configurada para gerar, na informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo, e

- a dita unidade de identificação de data e hora de transmissão é configurada para gerar informações de data e hora de transmissão, cada qual indicando a mesma data e hora em um bloco de criptografia imediatamente precedente a um bloco de criptografia para uma correspondente dentre a pluralidade de chaves de descriptografia de conteúdo.

7. Sistema de distribuição de conteúdo, incluindo um dispositivo servidor e um dispositivo terminal, em que o dito dispositivo servidor inclui:

- uma unidade de transmissão configurada para transmitir um conteúdo criptografado e informação relativa a conteúdo incluindo informações de data e hora de transmissão do conteúdo criptografado, e uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de geração de informação relacionada configurada para gerar, na informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de identificação de data e hora de transmissão configurada para gerar, na informação relativa a conteúdo, informações de data e hora de transmissão, cada qual indicando uma data e hora na qual a

informação relativa a conteúdo é transmitida; e

- uma unidade de criptografia de informação relacionada configurada para criptografar, em um modo de Encadeamento de Blocos Cifrados (CBC), a informação relativa a conteúdo na qual a pluralidade de chaves de descriptografia de conteúdo e informações de data e hora de transmissão foram geradas,

- a dita unidade de geração de informação relacionada é configurada para gerar, na informação relativa a conteúdo, a pluralidade de chaves de descriptografia de conteúdo, e

- a dita unidade de identificação de data e hora de transmissão é configurada para gerar informações de data e hora de transmissão, cada qual indicando a mesma data e hora em um bloco de criptografia imediatamente precedente a um bloco de criptografia para uma correspondente dentre a pluralidade de chaves de descriptografia de conteúdo, e

- em que o dito dispositivo terminal inclui:

- uma unidade de recebimento configurada para receber do dito dispositivo servidor:

(I) um conteúdo criptografado, e

(II) informações relativas a conteúdo incluindo (II-i) informações de data e hora de transmissão e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de obtenção de informação de hora configurada para obter informações de data e hora correntes, indicando uma data e hora correntes;

- uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e a hora indicada pelas informações de data e hora de transmissão recai dentro de uma faixa predeterminada, e julgar se o conteúdo está sendo recebido em tempo real quando a diferença de tempo recai dentro da faixa predeterminada; e

- uma unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a dita unidade de julgamento

de recepção em tempo real julga se o conteúdo está sendo recebido em tempo não real.

8. Método para usar o conteúdo de um sistema de distribuição de conteúdo incluindo um dispositivo servidor e um dispositivo terminal, o dito método compreendendo as etapas de:

- receber, do dito dispositivo servidor, (I) um conteúdo criptografado, e (II) informações relativas a conteúdo incluindo (II-i) informações de data e hora de transmissão e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- obter informação de hora e hora correntes indicando uma data e hora correntes; uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e a hora indicada pelas informações de data e hora de transmissão recai dentro de uma faixa predeterminada, e julgar se o conteúdo está sendo recebido em tempo real quando a diferença de tempo recai dentro da faixa predeterminada; e uma unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a dita unidade de julgamento de recepção em tempo real julga se o conteúdo está sendo recebido em tempo não real.

9. Produto de programa que faz com que um computador execute um método para usar um conteúdo em um sistema de distribuição de conteúdo incluindo um dispositivo servidor e um dispositivo terminal, o dito produto de programa fazendo com que o computador execute:

- o recebimento, do dito dispositivo servidor, (I) um conteúdo criptografado, e (II) informações relativas a conteúdo incluindo (II-i) informações de data e hora de transmissão e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- a obtenção de informação de data e hora correntes, indicando uma data e hora correntes;

- uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e a hora indicada pelas informações de

data e hora de transmissão recai dentro de uma faixa predeterminada, e julgar se o conteúdo está sendo recebido em tempo real quando a diferença de tempo recai dentro da faixa predeterminada; e

- uma unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a dita unidade de julgamento de recepção em tempo real julga se o conteúdo está sendo recebido em tempo não real.

10. Circuito integrado para um dispositivo terminal em um sistema de distribuição de conteúdo incluindo um dispositivo servidor e um dispositivo terminal, o dito circuito integrado compreendendo:

- uma unidade de recebimento configurada para receber, do dito dispositivo servidor, (I) um conteúdo criptografado, e (II) informações relativas a conteúdo incluindo (II-i) informações de data e hora de transmissão do conteúdo criptografado e (II-ii) uma pluralidade de chaves de descriptografia de conteúdo para descriptografar o conteúdo criptografado;

- uma unidade de obtenção de informação de hora configurada para obter informações de data e hora correntes, indicando uma data e hora correntes;

- uma unidade de julgamento de recepção em tempo real configurada para julgar se uma diferença de tempo entre uma hora indicada pela informação de data e hora correntes e uma hora indicada pelas informações de data e hora de transmissão recai dentro de uma faixa predeterminada, e julgar se o conteúdo está sendo recebido em tempo real quando a diferença de tempo recai dentro da faixa predeterminada; e

- uma unidade de controle de uso de conteúdo configurada para limitar o uso do conteúdo criptografado quando a dita unidade de julgamento de recepção em tempo real julga se o conteúdo está sendo recebido em tempo não real.

FIG. 1

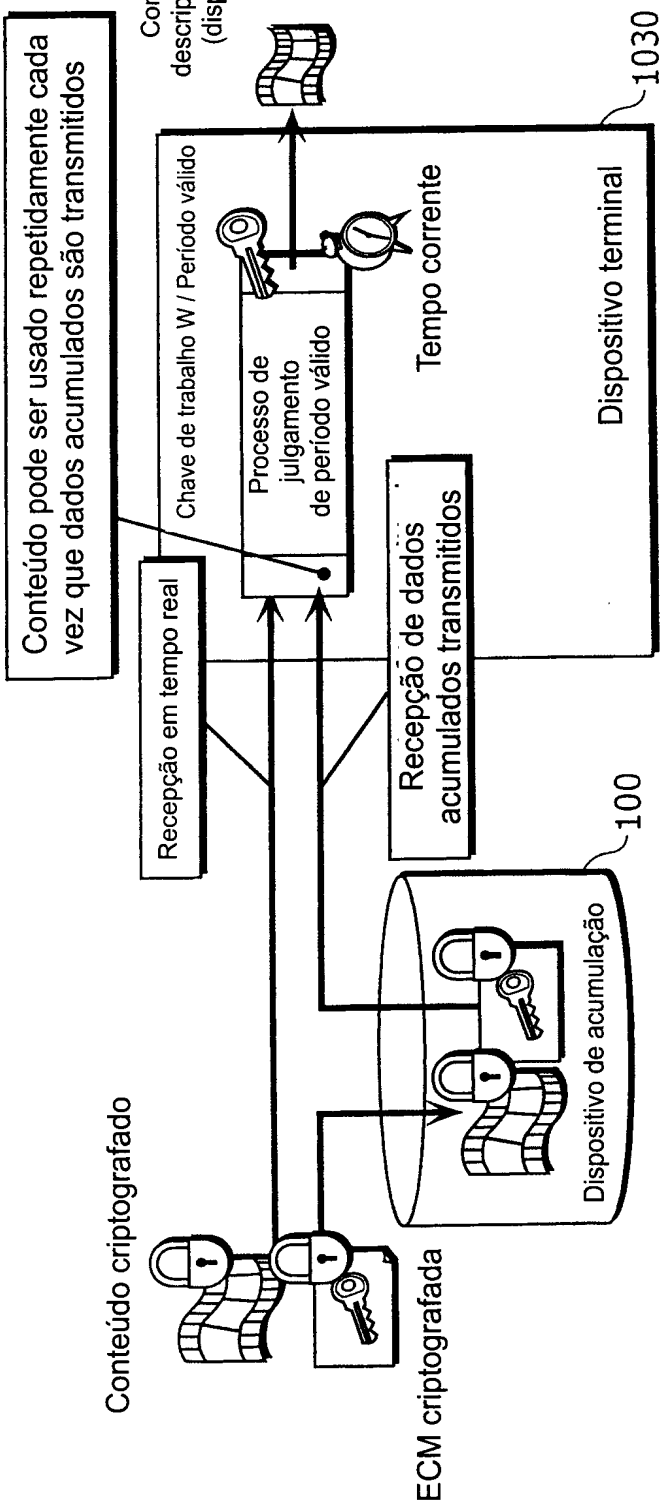

Conteúdo pode ser usado repetidamente cada vez que dados acumulados são transmitidos
Conteúdos descriptografados (disponíveis)
Chave de trabalho W / Período válido
Processo de julgamento de período válido
Tempo corrente
Dispositivo terminal
1030
Recepção em tempo real
Recepção de dados acumulados transmitidos
Dispositivo de acumulação
100
Conteúdo criptografado
ECM criptografada

FIG. 2

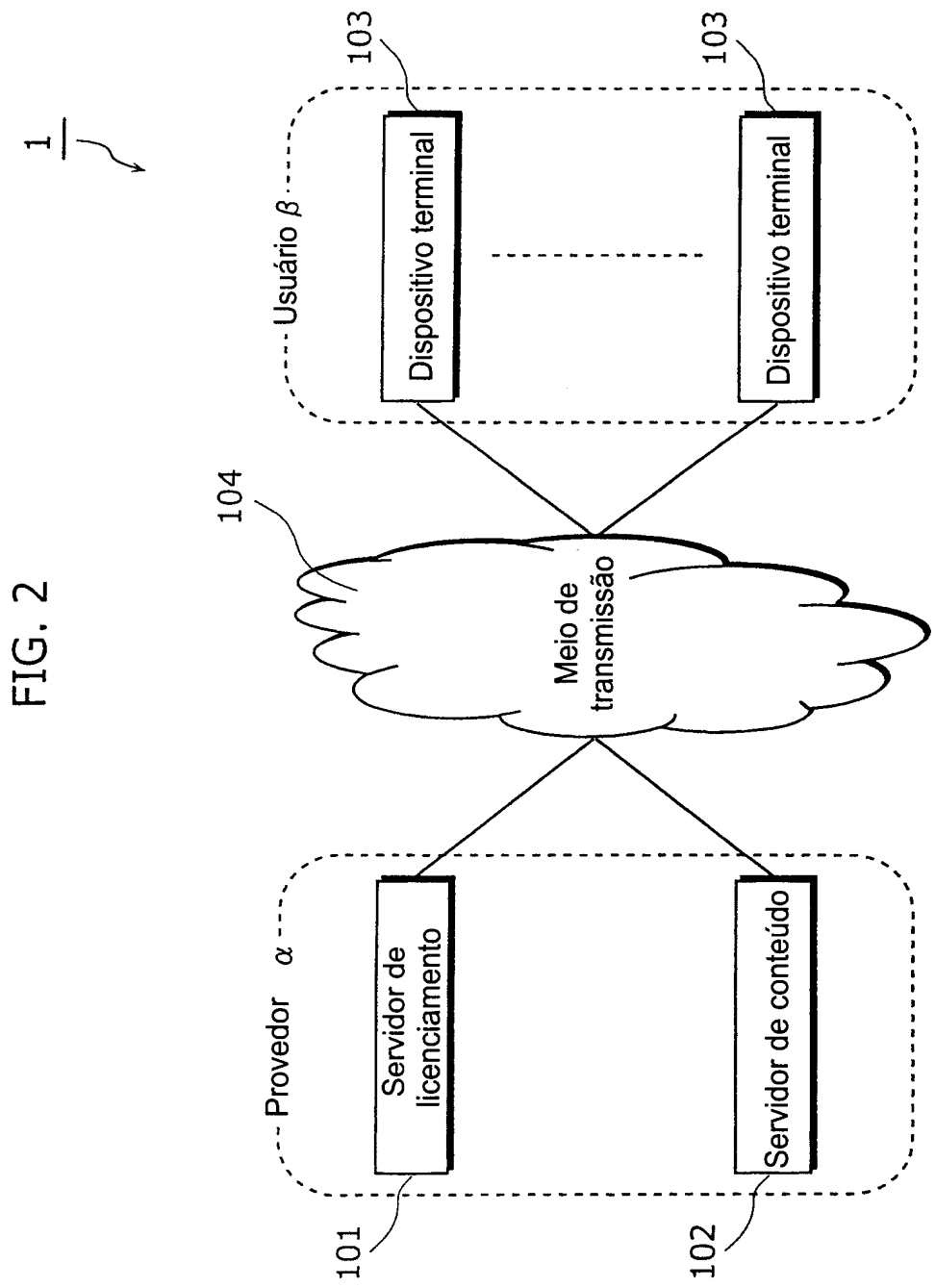

1
Usuário β
103
Dispositivo terminal
103
Dispositivo terminal
104
Meio de transmissão
Provedor α
Servidor de licenciamento
Servidor de conteúdo
101
102

FIG. 3

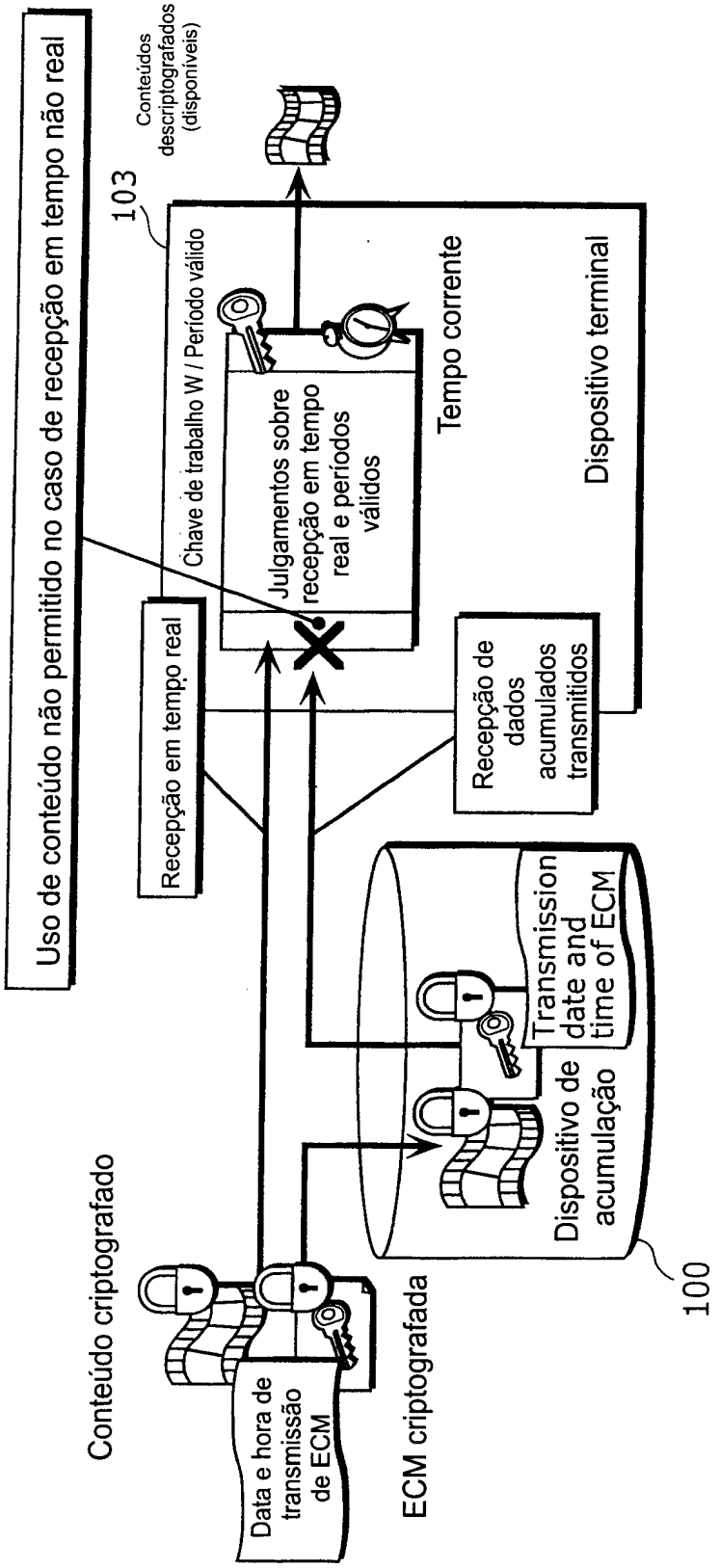

Uso de conteúdo não permitido no caso de recepção em tempo não real
Conteúdos descriptografados (disponíveis)
103
Chave de trabalho W / Período válido
Julgamentos sobre recepção em tempo real e períodos válidos
Tempo corrente
Dispositivo terminal
Recepção em tempo real
Recepção de dados acumulados transmitidos
Transmission date and time of ECM
Dispositivo de acumulação
100
Conteúdo criptografado
ECM criptografada
Data e hora de transmissão de ECM

FIG. 4

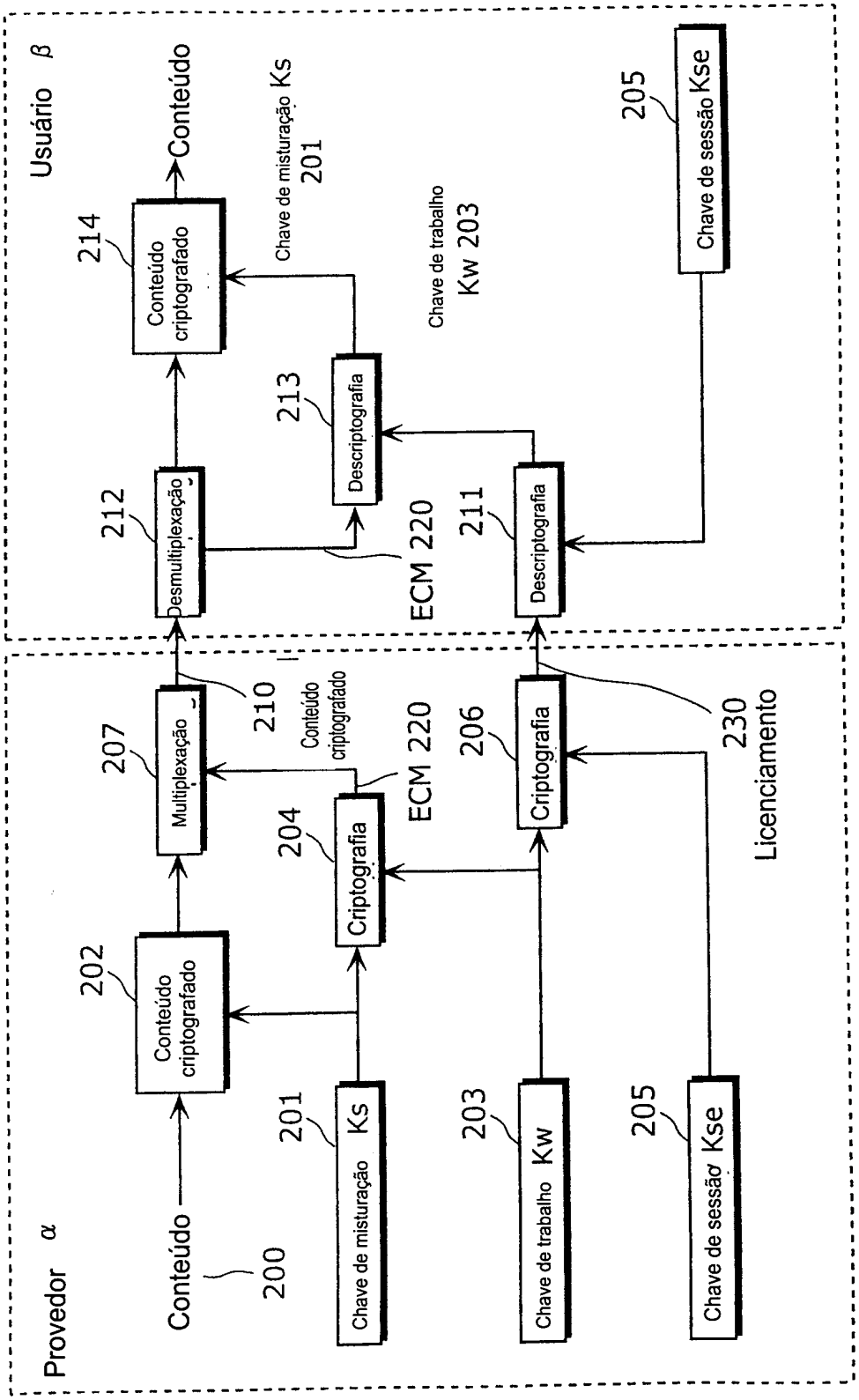

Provedor α
Usuário β
Conteúdo
200
Conteúdo criptografado
202
Chave de misturação Ks
201
Criptografia
204
Multiplexação
207
210
Conteúdo criptografado
ECM 220
Desmultiplexação
212
Descriptografia
213
Conteúdo criptografado
214
Conteúdo
Chave de misturação Ks
201
Chave de trabalho Kw
203
Criptografia
206
Descriptografia
211
ECM 220
Chave de trabalho Kw
203
Chave de sessão Kse
205
Chave de sessão Kse
205
230
Licenciamento

FIG. 5

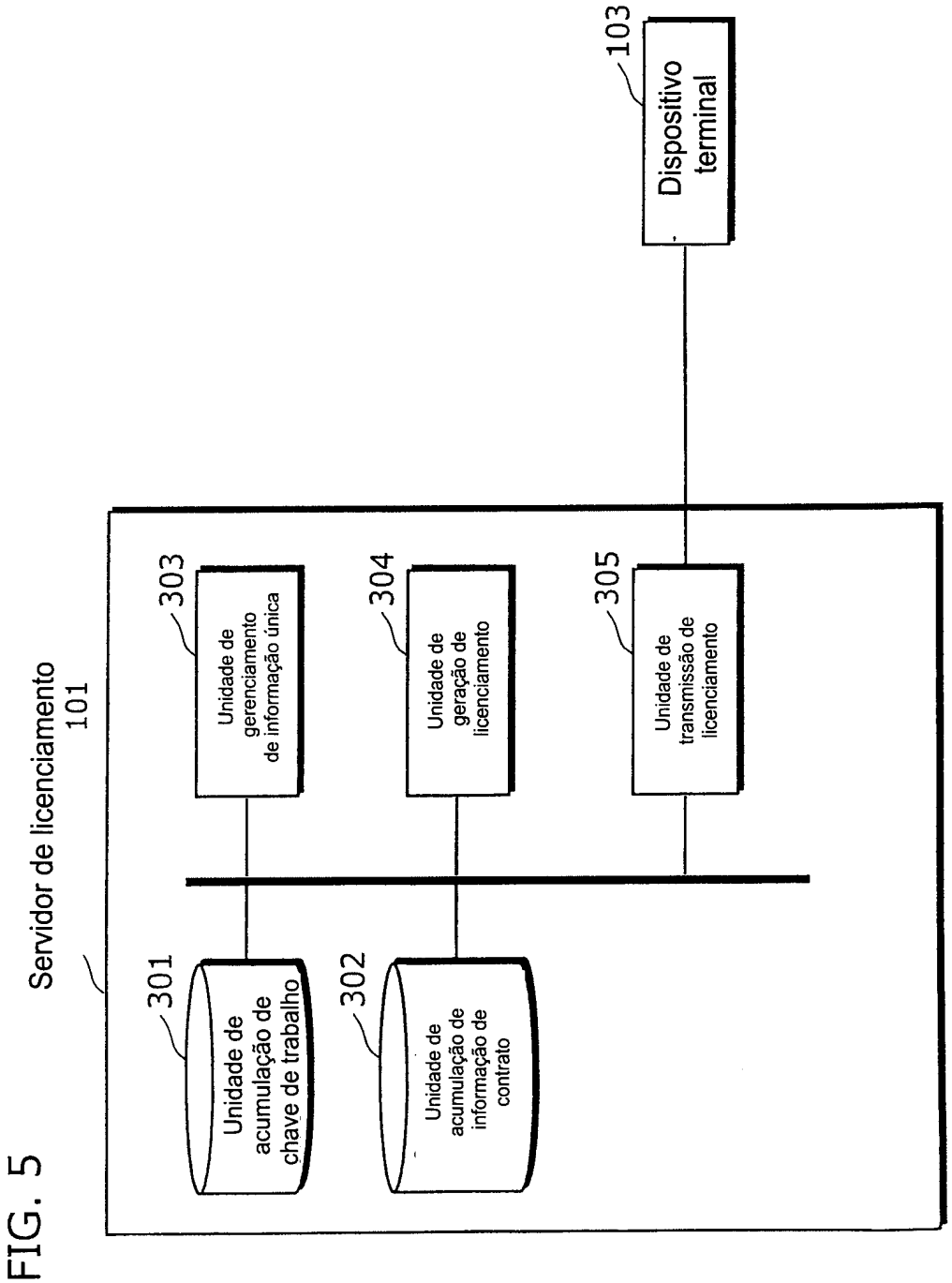

Servidor de licenciamento
101
Dispositivo terminal
103
Unidade de gerenciamento de informação única
303
Unidade de geração de licenciamento
304
Unidade de transmissão de licenciamento
305
Unidade de acumulação de chave de trabalho
301
Unidade de acumulação de informação de contrato
302

FIG. 6

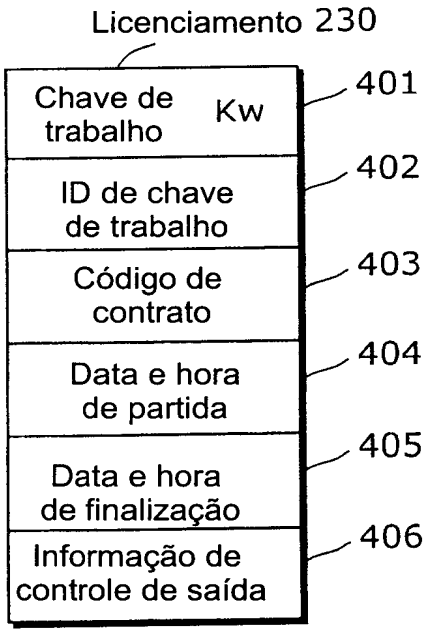

Licenciamento 230
Chave de trabalho Kw
401
ID de chave de trabalho
402
Código de contrato
403
Data e hora de partida
404
Data e hora de finalização
405
Informação de controle de saída
406

FIG. 7

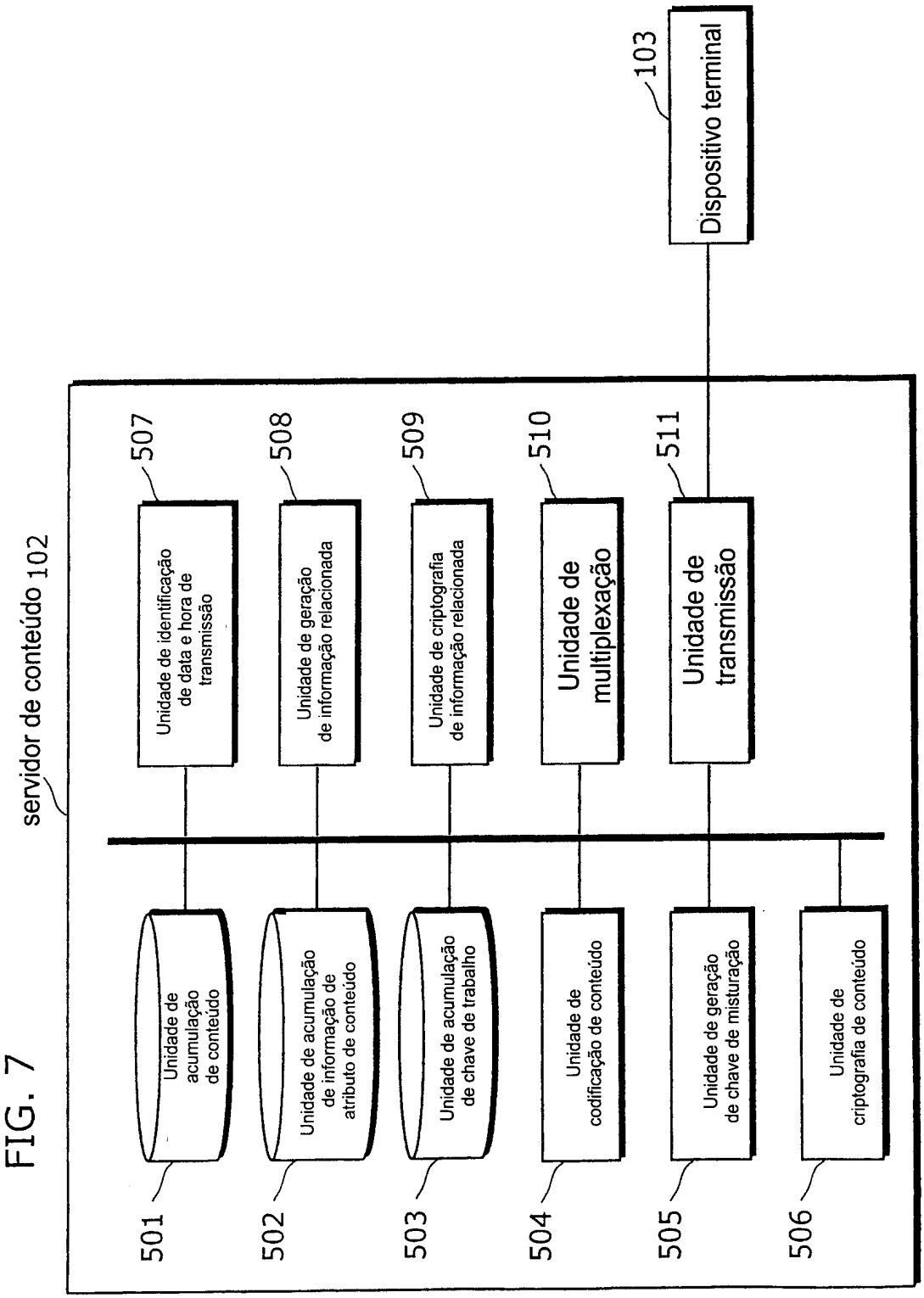

servidor de conteúdo 102
103
Dispositivo terminal
507
Unidade de identificação de data e hora de transmissão
508
Unidade de geração de informação relacionada
509
Unidade de criptografia de informação relacionada
510
Unidade de multiplexação
511
Unidade de transmissão
501
Unidade de acumulação de conteúdo
502
Unidade de acumulação de informação de atributo de conteúdo
503
Unidade de acumulação de chave de trabalho
504
Unidade de codificação de conteúdo
505
Unidade de geração de chave de misturação
506
Unidade de criptografia de conteúdo

FIG. 8A

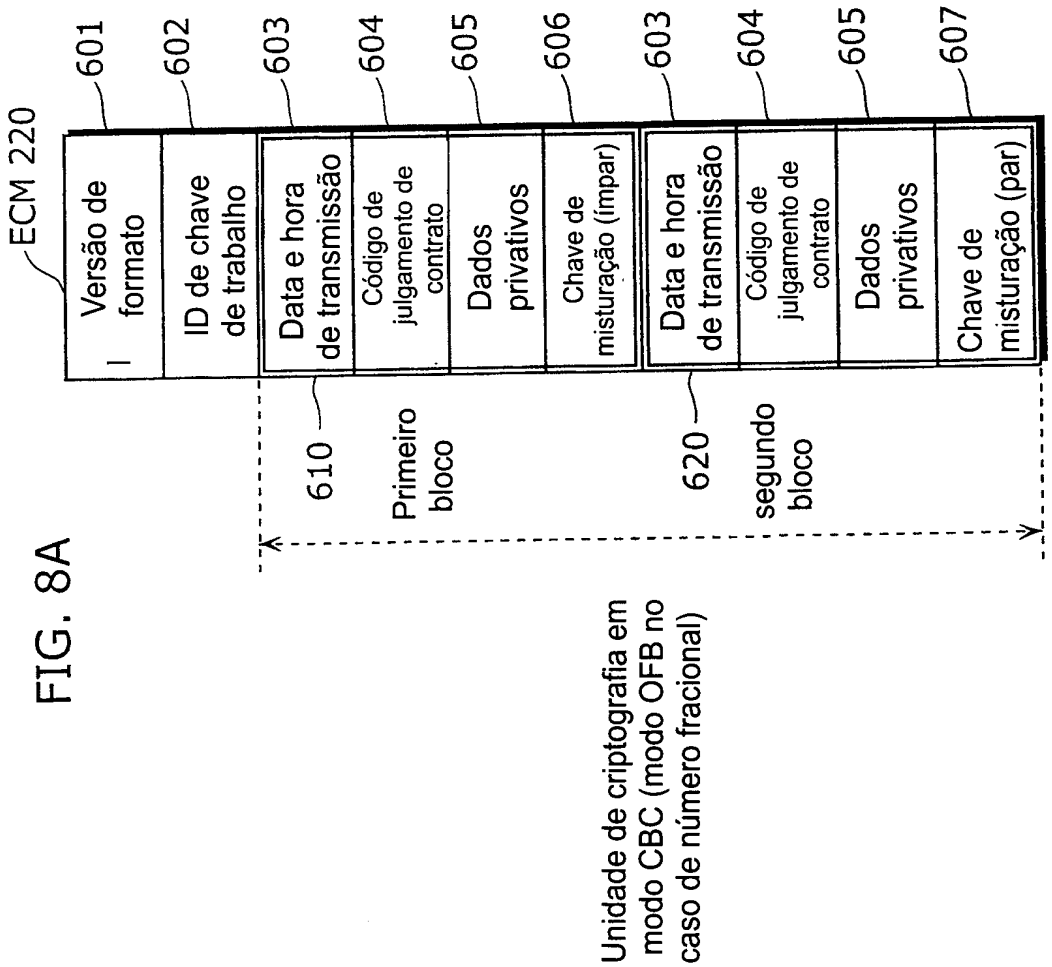

ECM 220
601
602
603
604
605
606
603
604
605
607
Versão de formato
ID de chave de trabalho
Data e hora de transmissão
Código de julgamento de contrato
Dados privativos
Chave de misturação (ímpar)
Data e hora de transmissão
Código de julgamento de contrato
Dados privativos
Chave de misturação (par)
610
Primeiro bloco
620
segundo bloco
Unidade de criptografia em modo CBC (modo OFB no caso de número fracional)

FIG. 8B

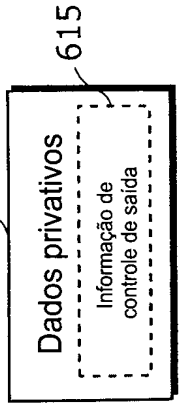

605
615
Dados privativos
Informação de controle de saída

FIG. 9

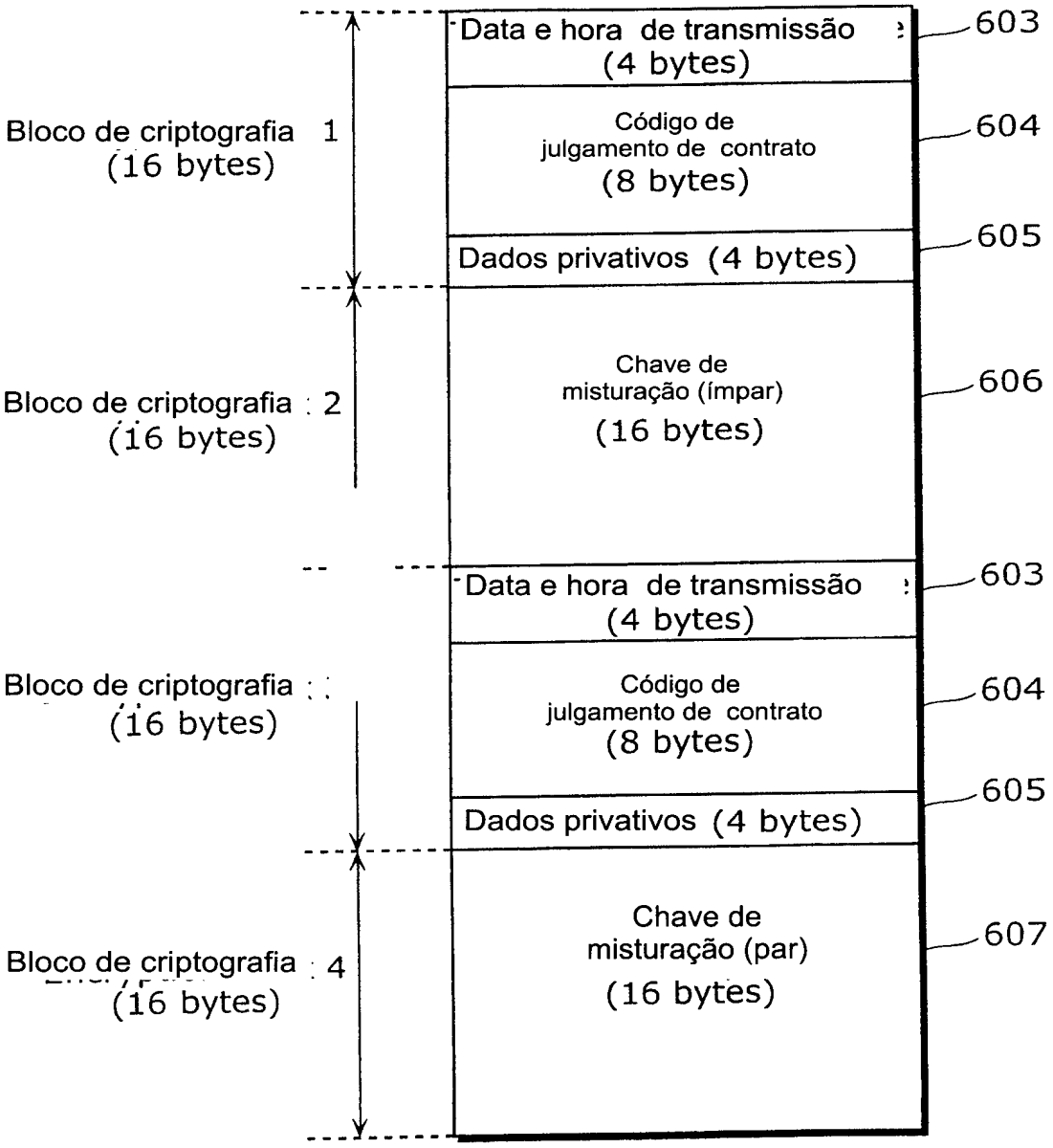

Bloco de criptografia 1
(16 bytes)
Data e hora de transmissão
(4 bytes)
603
Código de
julgamento de contrato
(8 bytes)
604
Dados privativos (4 bytes)
605
Bloco de criptografia 2
(16 bytes)
Chave de
misturação (ímpar)
(16 bytes)
606
Bloco de criptografia 3
(16 bytes)
Data e hora de transmissão
(4 bytes)
603
Código de
julgamento de contrato
(8 bytes)
604
Dados privativos (4 bytes)
605
Bloco de criptografia 4
(16 bytes)
Chave de
misturação (par)
(16 bytes)
607

FIG. 10

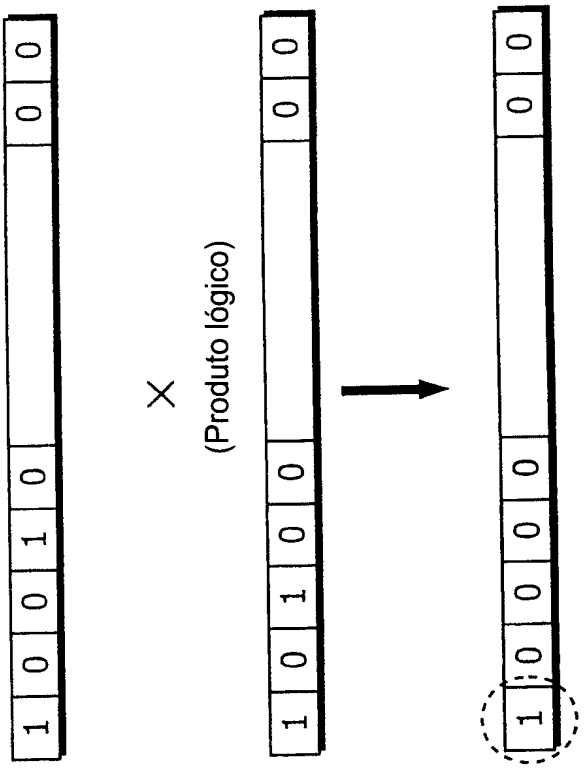

Código de contrato 403 :
1 0 0 1 0 0 0
×
(Produto lógico)
Código de julgamento de contrato 604 :
1 0 1 0 0 0 0
1 0 0 0 0 0 0

FIG. 11

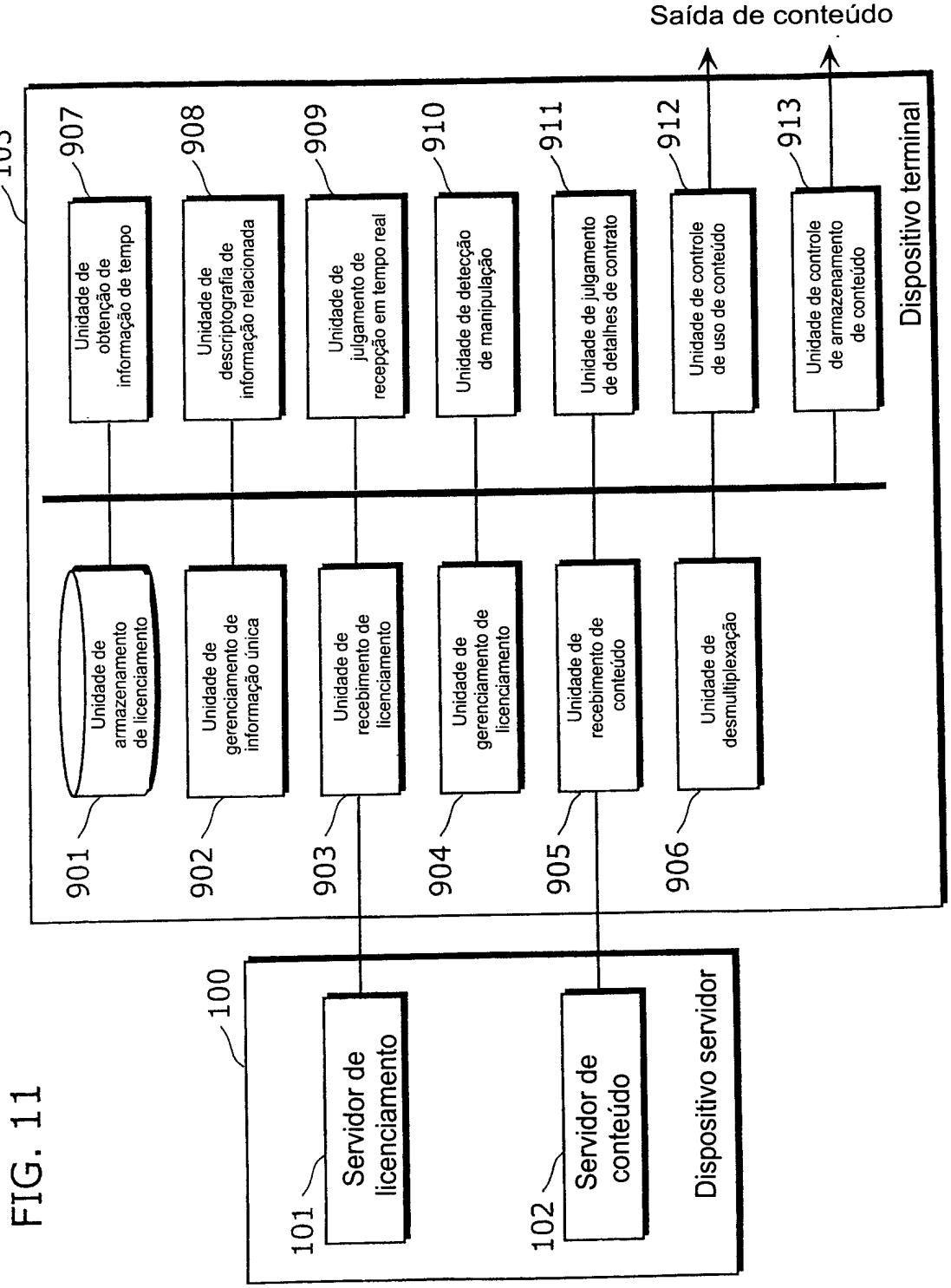

Saída de conteúdo
103
907
908
909
910
911
912
913
Unidade de obtenção de informação de tempo
Unidade de descriptografia de informação relacionada
Unidade de julgamento de recepção em tempo real
Unidade de detecção de manipulação
Unidade de julgamento de detalhes de contrato
Unidade de controle de uso de conteúdo
Unidade de controle de armazenamento de conteúdo
Dispositivo terminal
Unidade de armazenamento de licenciamento
Unidade de gerenciamento de informação única
Unidade de recebimento de licenciamento
Unidade de gerenciamento de licenciamento
Unidade de recebimento de conteúdo
Unidade de desmultiplexação
901
902
903
904
905
906
100
Servidor de licenciamento
Servidor de conteúdo
Dispositivo servidor
101
102

FIG. 12

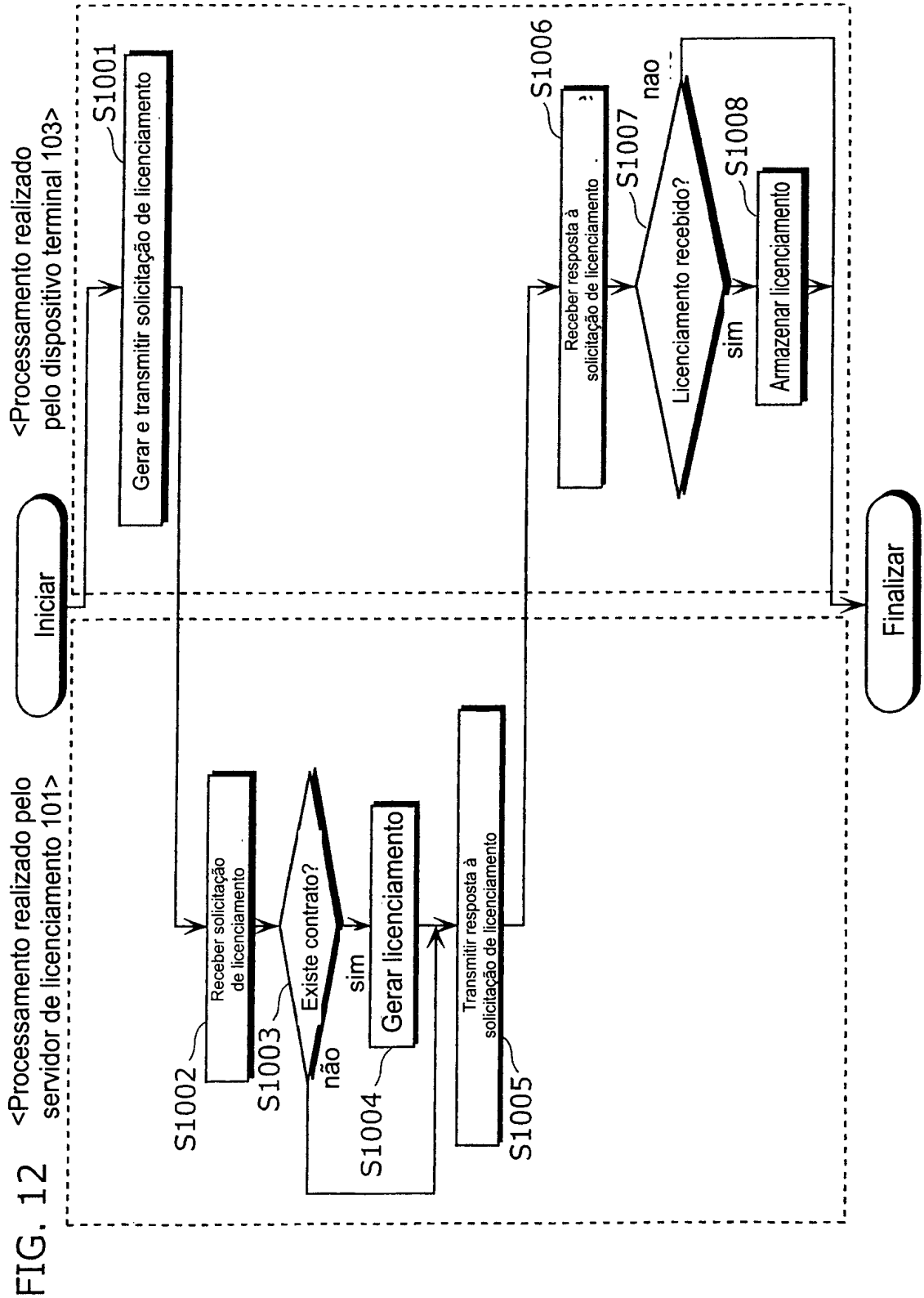

<Processamento realizado pelo servidor de licenciamento 101>
<Processamento realizado pelo dispositivo terminal 103>
Iniciar
S1001
Gerar e transmitir solicitação de licenciamento
S1002
Receber solicitação de licenciamento
S1003
Existe contrato?
não
sim
S1004
Gerar licenciamento
S1005
Transmitir resposta à solicitação de licenciamento
S1006
Receber resposta à solicitação de licenciamento
S1007
Licenciamento recebido?
nao
sim
S1008
Armazenar licenciamento
Finalizar

FIG. 13

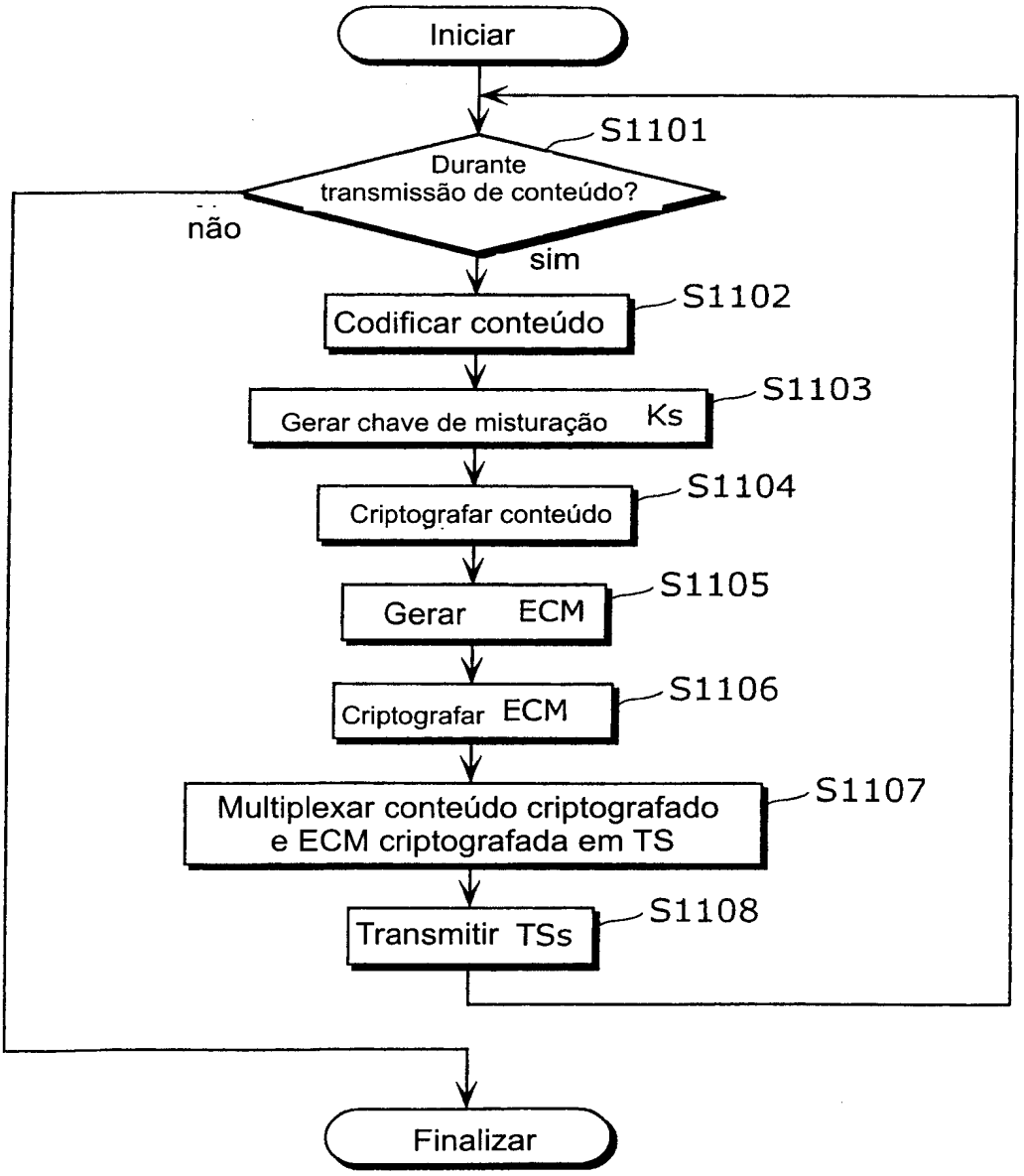

Iniciar
S1101
Durante transmissão de conteúdo?
não
sim
S1102
Codificar conteúdo
S1103
Gerar chave de misturação Ks
S1104
Criptografar conteúdo
S1105
Gerar ECM
S1106
Criptografar ECM
S1107
Multiplexar conteúdo criptografado e ECM criptografada em TS
S1108
Transmitir TSs
Finalizar

FIG. 14

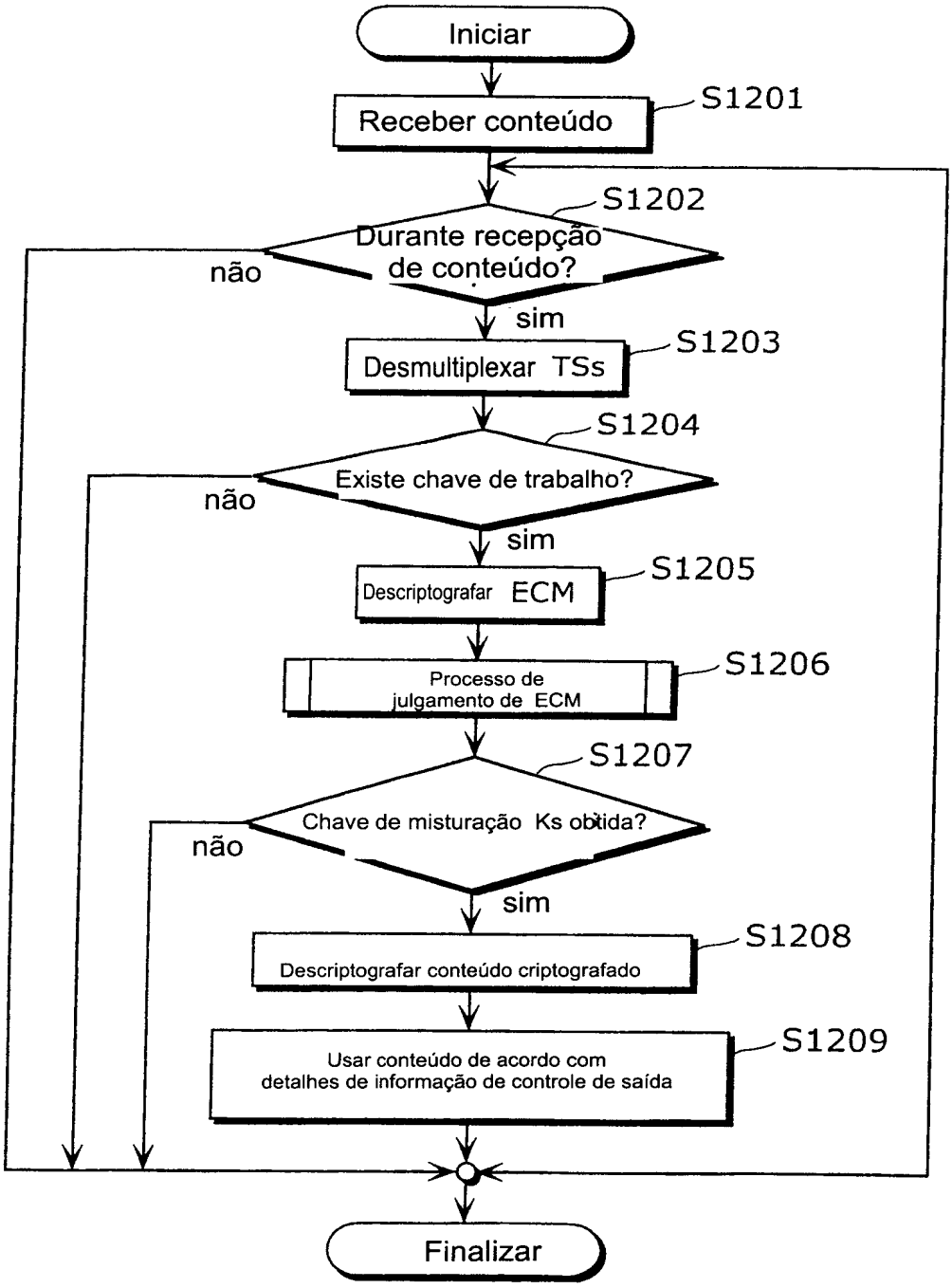

Iniciar
Receber conteúdo
S1201
S1202
Durante recepção de conteúdo?
não
sim
Desmultiplexar TSs
S1203
S1204
Existe chave de trabalho?
não
sim
Descriptografar ECM
S1205
Processo de julgamento de ECM
S1206
S1207
Chave de misturação Ks obtida?
não
sim
Descriptografar conteúdo criptografado
S1208
Usar conteúdo de acordo com detalhes de informação de controle de saída
S1209
Finalizar

FIG. 15

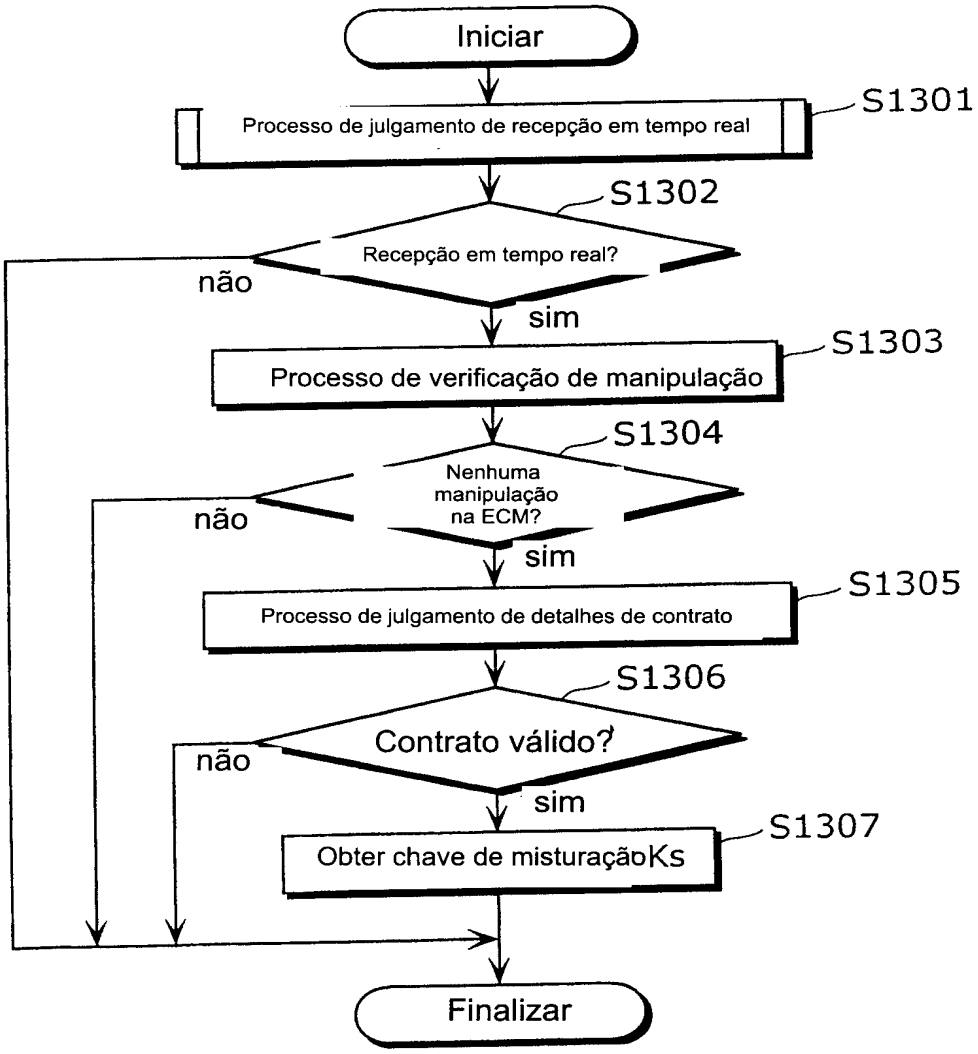

Iniciar
Processo de julgamento de recepção em tempo real
S1301
S1302
Recepção em tempo real?
não
sim
Processo de verificação de manipulação
S1303
S1304
Nenhuma manipulação na ECM?
não
sim
Processo de julgamento de detalhes de contrato
S1305
S1306
Contrato válido?
não
sim
Obter chave de misturação Ks
S1307
Finalizar

FIG. 16

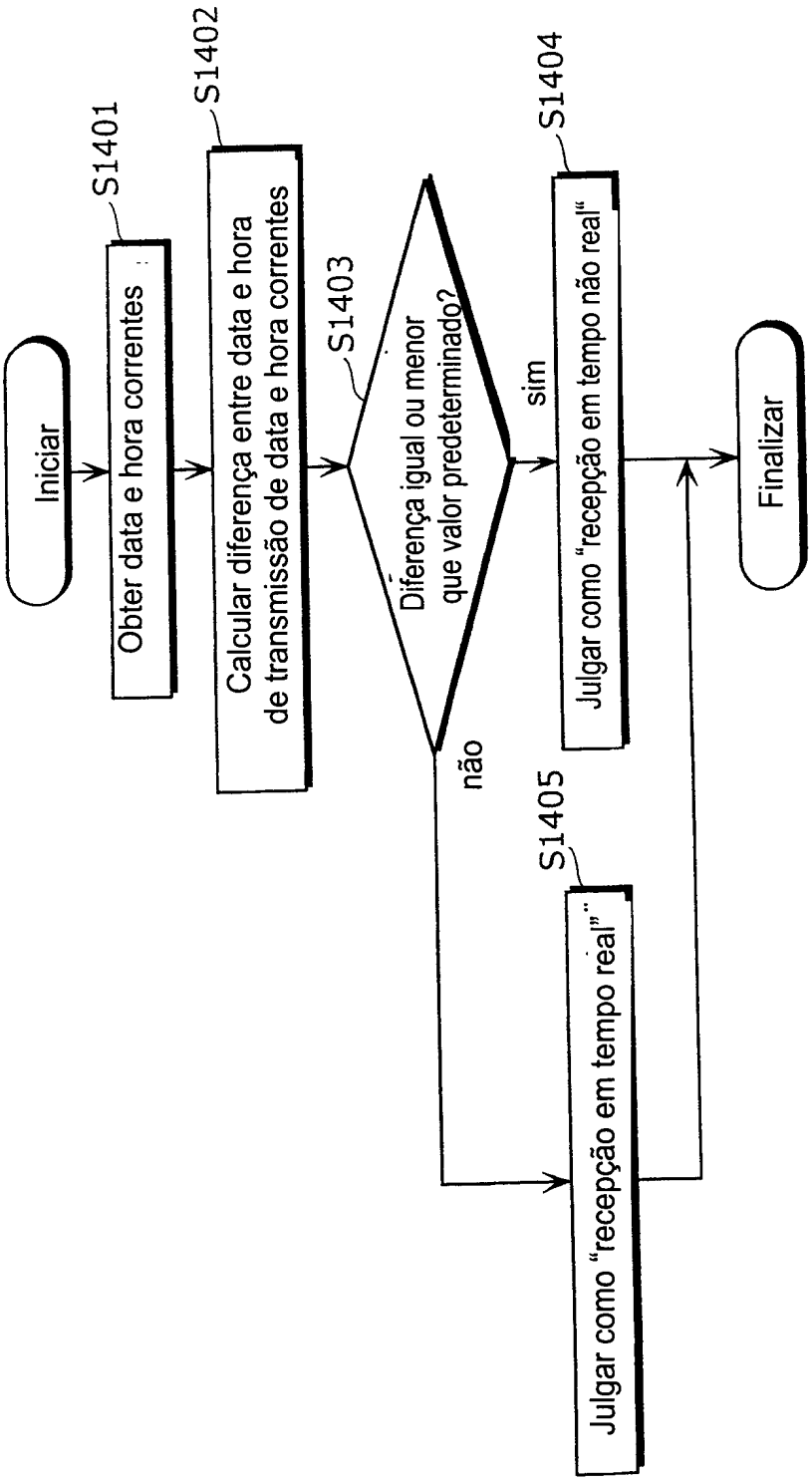

Iniciar
S1401
Obter data e hora correntes
S1402
Calcular diferença entre data e hora de transmissão de data e hora correntes
S1403
Diferença igual ou menor que valor predeterminado?
sim
não
S1404
Julgar como "recepção em tempo não real"
S1405
Julgar como "recepção em tempo real"
Finalizar

FIG. 17

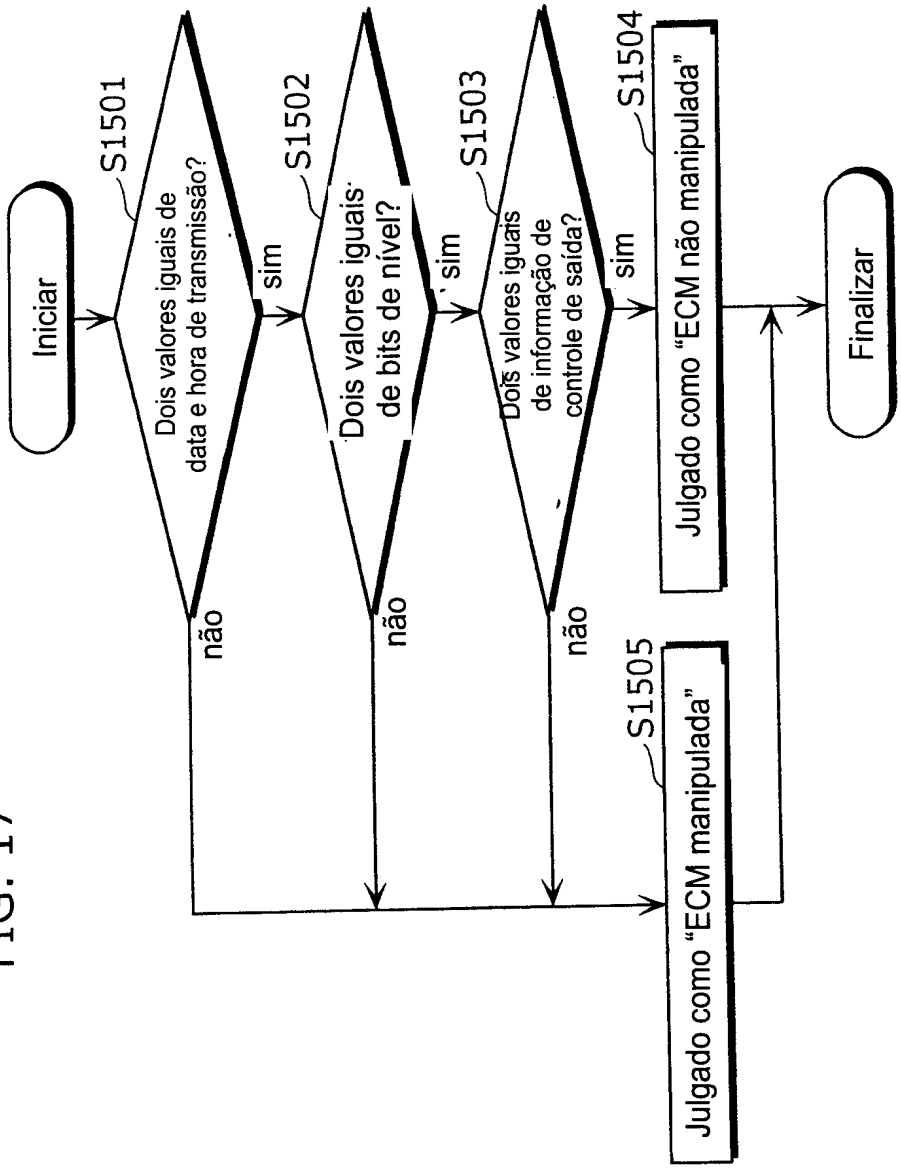
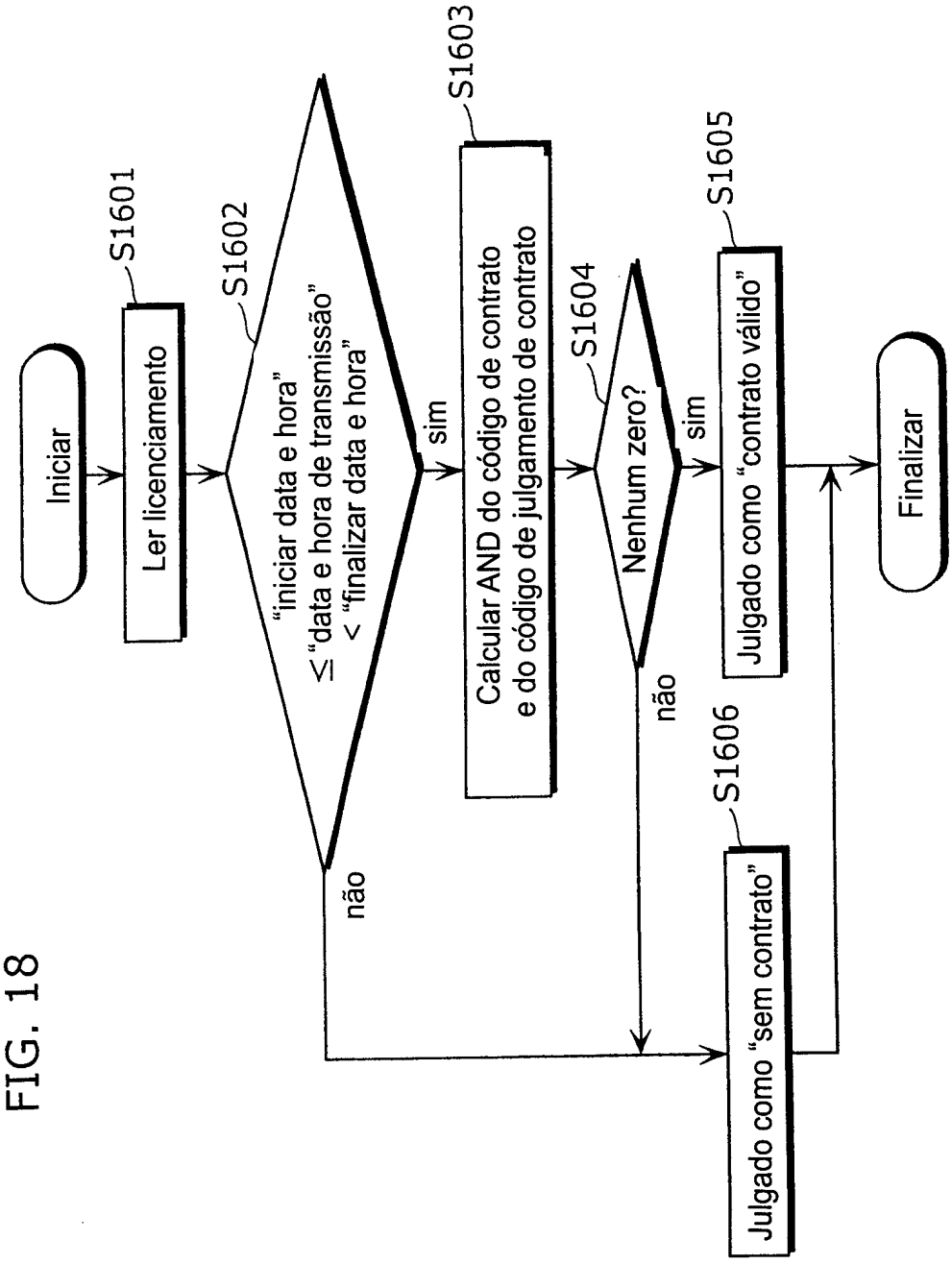

Iniciar
S1501
Dois valores iguais de data e hora de transmissão?
sim
não
S1502
Dois valores iguais de bits de nível?
sim
não
S1503
Dois valores iguais de informação de controle de saída?
sim
não
S1504
Julgado como "ECM não manipulada"
S1505
Julgado como "ECM manipulada"
Finalizar

FIG. 18


Iniciar
S1601
Ler licenciamento
S1602
"iniciar data e hora"
≤ "data e hora de transmissão"
< "finalizar data e hora"
sim
não
S1603
Calcular AND do código de contrato
e do código de julgamento de contrato
S1604
Nenhum zero?
sim
não
S1605
Julgado como "contrato válido"
S1606
Julgado como "sem contrato"
Finalizar

RESUMO

Patente de Invenção: **"DISPOSITIVO TERMINAL, DISPOSITIVO SERVIDOR, E SISTEMA DE DISTRIBUIÇÃO DE CONTEÚDO".**

A fim de prover um sistema de distribuição de conteúdo que possa impedir o uso de um conteúdo que foi temporariamente acumulado após o período válido.

Um sistema de distribuição de conteúdo (1) incluindo um servidor de licenciamento (101) que emite um licenciamento, um servidor de conteúdo (102) que transmite o conteúdo, um dispositivo terminal (103) que controla o uso do conteúdo com base no licenciamento emitido. O dispositivo terminal (103) não permite o uso do conteúdo criptografado recebido quando é julgado que o conteúdo criptografado recebido do servidor de conteúdo (102) não é o conteúdo recebido em tempo real.