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

(21) **PI0620700-6 A2**

BRPI0620700A2

(22) Data de Depósito: 13/12/2006
(43) Data da Publicação: 06/12/2011
(RPI 2135)

(51) Int.Cl.:
H04N 7/167

(54) Título: MÉTODO PARA CODIFICAÇÃO E DECODIFICAÇÃO DE UM CONTEÚDO DE ACESSO CONDICIONAL

(30) Prioridade Unionista: 15/12/2005 EP 052927019

(73) Titular(es): NAGRA FRANCE SAS

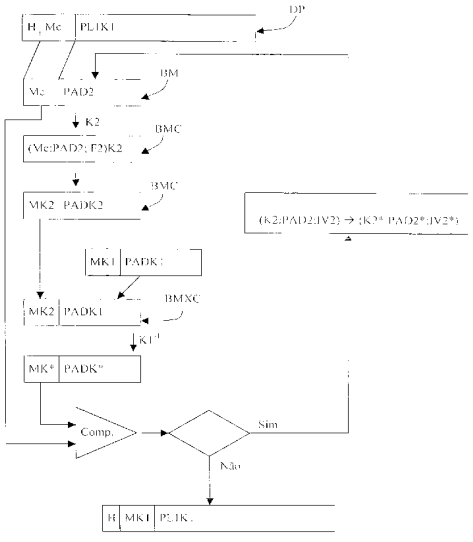
(72) Inventor(es): Pascal Junod, Thierry Lelegard

(74) Procurador(es): MARCAS MARCANTES E PATENTES LTDA

(86) Pedido Internacional: PCT EP2006069660 de 13/12/2006

(87) Publicação Internacional: WO 2007/068720de 21/06/2007

(57) Resumo: MÉTODO PARA CODIFICAÇÃO E DECODIFCAÇÃO DE UM CONTEÚDO DE ACESSO CONDICIONAL. Esta invenção é relativa ao método de codificação e decodificação para um conteúdo de acesso condicional. no qual o conteúdo é transmitido na forma de pacotes de dados (DP). os pacotes anteriores sendo codificados por uma primeira chave (K1) associada a um primeiro valor de enchimento (PAD 1) e a um primeiro elemento de enchimento codificado (PADK1) e os pacotes seguintes sendo codificado por uma secunda chave (K2) associada a um segundo valor de enchimento (PAD2) e a um segundo elememo de enchimento codificado (PADK2). Neste método. a primeira chave (K1) e o primeiro valor de enchimento (PAD1) formam um primeiro conjunto de parametros de coditicacão. a segunda chave (K2) e o segundo valor de enchimento formando um segundo conjunto de parametros de codificação. Este método inclui as etapas de (a) extração de marcador (Mc) de um pacote de dados (DP):(b) criação de um primeiro bloco de marcação incluindo um marcador (Mc) e o secundo valor de enchimento (PAD2); (c) codificacão do primeiro bloco de marcação com a segunda chave de codificação (K2); (d) extração de um segundo valor de marcação codificação (MK2) do primeiro bloco de marcação codificado: (e) criação de um bloco de marcação misto incluindo um segundo valor de marcação codificado (MK2) e um primeiro elemento de enchimento codificado (PADK 1); (f) decodificacão do bloco de marcacão misto por meio da primeira chave de codificação (K1), a fim de obter um bloco de marcação misto decodificado; (g) extração de uma parte predeterminada do bloco de marcação misto decodificado; (h) comparação desta parte extraída com um valor de referência (Mc; PDV2); (i) se a comparação levar a igualdade, determinação de uma novo conjunto de parâmetros de codificação diferente do primeiro conjunto de parâmetros de codificação e repetição das etapas b) a h), nas quais o segundo conjunto de parâmetros de codificação é substituido pelo novo segundo conjunto de parâmetros de codificação.



MÉTODO PARA CODIFICAÇÃO E DECODIFICAÇÃO DE UM CONTEÚDO DE ACESSO CONDICIONAL

Campo Técnico

Esta invenção é relativa ao método de codificação e decodificação para conteúdo de acesso condicional, no qual este conteúdo é enviado na forma de pacotes de dados.

Este método é aplicado, em particular, a televisão por assinatura, mas também a outras configurações, nas quais dados são enviados de forma codificada. Estes dados podem, em particular, envolver transações financeiras, software, jogos ou conteúdo musical, por exemplo, ou informação, tal como informação sobre bolsa de valores, previsões do tempo ou semelhante.

Estado da Técnica

Em certo número de aplicativos, em particular no campo da televisão por assinatura, dados que formam um conteúdo são enviados na forma de pacotes de dados. Estes pacotes podem, em particular, ter uma extensão fixada predefinida. Estes pacotes são geralmente transmitidos de maneira codificada destinados para um conjunto de receptores, tais como decodificadores.

Em paralelo aos pacotes de dados, informação decodificada também é transmitida. Em particular, esta informação contém chaves de decodificação ou dados que permitem a determinação das chaves necessárias. A fim de garantir certo nível de segurança no sistema de dados de acesso condicional, é imperativo que as chaves sejam mudadas após certo uso ou período de validade. Na prática, no caso particular da televisão por assinatura, uma chave poderia ser usada para acessar um conteúdo de televisão por poucos segundos, ou até mesmo por alguns minutos. Uma das limitações relativas à mudança da chave é a necessidade de associar a chave de decodificação correta com cada pacote de dados. Caso contrário, estes dados não serão acessíveis. Entretanto, é praticamente impossível sincronizar os dados com a informação de decodificação, em particular, devido ao trabalho interno dos sistemas.

Por esta razão, é necessário dispor de um mecanismo que permita para cada pacote de dados ser associado com a chave de decodificação correspondente, sem ter de sincronizar estes dois elementos.

De acordo com um conhecido método de realização, os pacotes de dados geralmente contém um marcador com um valor sabido que permite ao receptor/decodificador localizar o começo de um pacote e processar este do modo devido.

De acordo com os padrões utilizados para a formatação destes pacotes, a extensão de um pacote é fixada e não é possível adicionar dados suplementares aos já existentes. Em particular, isto significa que quando a chave de codificação de um pacote é modificada, é impossível indicar esta chave mudada no pacote, por exemplo, por meio de uma informação de mudança de chave. Deve ser notado que a mudança das chaves não é sincronizada com os pacotes, de tal maneira que uma chave pode ser utilizada para codificar ou decodificar vários pacotes.

Na prática, na recepção de um pacote, este último é decodificado com a chave atual.

É então verificado se o resultado da decodificação é utilizável, quer dizer, se contém o marcador. Se este não for o caso, o mesmo pacote é decodificado com a chave seguinte. Se o resultado desta decodificação for utilizável e, deste modo, contiver o marcador, a nova chave é usada para decodificação. Se o resultado desta decodificação não contiver o marcador, uma mensagem de erro é gerada.

Esta modalidade apresenta uma importante desvantagem. Na verdade, acontece que a decodificação de um pacote com uma chave atual fornece um resultado contendo o marcador, até mesmo por este pacote ter sido codificado com uma outra chave, a não ser a atual. Este resultado dado casualmente é produzido de acordo com uma freqüência significante e impede um usuário de acessar os conteúdos mesmo se ele tiver os direitos.

Esta invenção propõe evitar esta desvantagem por executar um método, no qual a decodificação com uma chave, de um pacote codificado por uma chave diferente nunca conter o marcador. Portanto, é impossível confundir duas chaves de codificação e acesso ao conteúdo é, desde modo, sempre assegurado.

Descrição da Invenção

O objetivo da invenção é alcançado por um método de codificação e decodificação para conteúdo de acesso condicional, no qual dito conteúdo é transmitido na forma de pacotes de dados (DP), sendo os pacotes anteriores codificados por uma primeira chave (K1) associada a um primeiro valor de enchimento (PAD1) e a um primeiro elemento de enchimento codificado (PADK1) e os pacotes seguintes sendo codificados por uma segunda chave (K2) associada a um segundo valor de enchimento (PAD2) e a um segundo elemento de enchimento codificado (PADK2), no qual ao menos a primeira chave (K1) e o primeiro valor de enchimento (PAD1) formam um primeiro conjunto de parâmetros de codificação e, no qual, pelo menos a segunda chave (K2) e o segundo valor de enchimento formam um segundo conjunto de parâmetros de codificação. Este método compreende as seguintes etapas:

a) extração de um marcador (Mc) de um pacote de dados (DP);

b) criação de um primeiro bloco de marcação, incluindo, de um lado o marcador (Mc) e, de outro lado o segundo valor de enchimento (PAD2);

c) codificação do primeiro bloco de marcação com a segunda chave de codificação (K2);

d) extração de um segundo valor de marcação codificado (MK2) do primeiro bloco de marcação codificado;

e) criação de um bloco de marcação misto incluindo de um lado o segundo valor de marcação (MK2) e, de outro lado o primeiro valor de enchimento (PADK1);

f) decodificação do bloco de marcação por meio da primeira chave de codificação (K1), a fim de obter um bloco de marcação misto decodificado;

g) extração de uma parte predeterminada de um bloco de marcação misto decodificado;

h) comparação desta parte extraída com um valor de referência (Mc; PDV2);

i) se a comparação levar a uma igualdade, determinação de um novo conjunto de parâmetros de codificação diferente do primeiro conjunto de parâmetros de codificação e repetição das etapas b) a h), nas quais o segundo conjunto de parâmetros de codificação é substituído por um novo segundo conjunto de parâmetros de codificação.

Em um sistema de televisão por assinatura utilizando o método da invenção, os pacotes de dados podem ser transmitidos a um grupo de receptores, enviados de ponto a ponto ou podem ser armazenados em um suporte físico, tal como um disco rígido, por exemplo. A decodificação de dados pode também ser transmitida, enviada ponto a ponto ou armazenada. Geralmente, o dispositivo de decodificação dentro do receptor ou do decodificador, dispõe simultaneamente de dois pedaços de informação de decodificação. Quando estes pedaços de informação são armazenados na memória do decodificador, eles são transmitidos ao dispositivo de decodificação, de tal modo que eles apenas dispõem dos dois pedaços de informação ao mesmo tempo. Os remanescentes são armazenados para uso subseqüente. Se estes pedaços de informação são as chaves de decodificação, eles dispõem em geral da chave atual e da chave seguinte, quer dizer, a chave que tem servido para codificar o pacote durante a visualização e a chave que tem servido para codificar o próximo pacote utilizando uma chave diferente da chave atual.

Embora o pacote de dados, devido a sua estrutura e as limitações relativas aos padrões utilizados, não permitir a inclusão de informação da mudança de chave, o método da invenção determina para qual pacote a próxima chave deve ser utilizada.

Na verdade, na invenção, enquanto um pacote de dados é acessado, o pacote seguinte é decodificado com a chave atual. Neste pacote decodificado, é determinado se ele

contém um marcador. Se este não for o caso, a chave seguinte é utilizada para decodificar o pacote de dados. Se esta chave seguinte tiver sido usada para codificar este pacote, então esta chave é utilizada. Dita chave se torna a nova chave atual. Então, uma outra chave seguinte é carregada.

Se o marcador é encontrado após a decodificação do pacote com a chave atual, pode ser suposto que a chave atual é aquela que tenha sido utilizada para codificar o pacote em questão. Entretanto, a fim de evitar este marcador de estar presente aleatoriamente, mesmo embora a chave seguinte tenha sido utilizada para codificar o pacote em questão, no momento da codificação, um teste é executado. O objetivo deste teste é assegurar que é impossível encontrar um marcador após a decodificação, por certa chave, de um pacote que tenha sido codificado por outra chave "temporariamente adjacente", quer dizer, seguinte ou anterior.

Isto não pode ser garantido pelos métodos do estado da técnica. Na verdade, como indicado anteriormente, um pacote de dados contém, em particular, um marcador e uma parte funcional, o marcador sendo fixado e a parte funcional sendo variável. Como esta parte funcional é variável, é impossível garantir que se o pacote é codificado com uma chave, então este pacote é decodificado com uma outra chave. O pacote obtido não contém um marcador.

Nesta invenção, graças ao teste, é possível ter certeza que se o marcador é encontrado no pacote decodificado, então a decodificação tenha sido executada com a chave correta.

Breve Descrição dos Desenhos

Esta invenção e suas vantagens serão melhor compreendidas com referência aos desenhos incluídos e a descrição detalhada de uma modalidade particular, na qual:

- Figuras 1a a 1g mostram esquematicamente a codificação de um pacote de dados, de acordo com o método da invenção;

- Figura 2 mostra uma primeira modalidade da verificação dos parâmetros utilizados para a codificação;

- Figura 3 mostra uma segunda modalidade de verificação dos parâmetros utilizados para a codificação;

- Figuras 4a a 4g representam a decodificação de um bloco de dados por meio da chave correta; e

- Figuras 5a a 5d ilustram a decodificação de um bloco por meio de uma chave falsa.

Melhor Modo de Executar a Invenção

Com referência as figuras 1a a 1g, o conteúdo de transmissão é transmitido na forma de pacotes de dados DP. Cada pacote de dados é formado de um cabeçalho H no espaço livre, de um marcador Mc e de uma parte funcional PL. O cabeçalho H contém informação de serviço, bem como um indicador de início do pacote. De acordo com uma modalidade particular, é formado de 4 bytes e está sempre no espaço livre. O marcador Mc é estável em todos os pacotes. Na prática, é geralmente formado de três bytes onde os dois primeiros têm o valor 0 e o terceiro tem o valor 1. Nos desenhos, a parte funcional PL tem a referência 1 para este primeiro pacote. É formado com seu próprio acesso condicional de dados, quer dizer, dados de áudio ou vídeo, por exemplo, no caso de transmissão de conteúdo de televisão por assinatura ou música.

O tamanho do pacote de dados DP completo é fixado e não deve ser modificado. Na prática, pode ser, por exemplo, de 188 bytes.

Pela aplicação do método da invenção, em primeiro lugar, o marcado é extraído do primeiro pacote de dados DP. Um bloco é então formado, chamado de primeiro bloco de marcação BM. Este bloco de marcação inclui de um lado o marcador Mc e de outro um primeiro valor de enchimento PAD1. Este valor de enchimento pode ser escolhido

aleatoriamente de uma lista predeterminada ou pode ser estável. A importância deste valor de enchimento é descrito abaixo, em detalhes.

No método da invenção, geralmente um algoritmo de codificação em bloco é utilizado. Neste tipo de algoritmo, o tamanho dos blocos utilizados é fixado e pode ser, por exemplo, de 8 ou 16 bytes, ainda que outros valores sejam possíveis. Este tamanho é chamado daqui por diante de tamanho de codificação. O tamanho do primeiro valor de enchimento PAD1 é tal que o tamanho do bloco de marcação BM é igual ao tamanho de codificação.

O marcador de bloco BM é então codificado com a primeira chave de codificação K1, a fim de obter um bloco de marcação codificado BMC. Este é cortado em duas partes, uma delas possui o tamanho do marcador Mc e outra parte possui o tamanho restante. A parte que possui o tamanho do marcador tem a referência MK1 na figura 1d e é chamada de valor de marcação codificado. A outra parte possui a referência PADK1 e é chamada de elemento de enchimento codificado. O local onde o bloco de marcação codificado é cortado depende do tamanho do marcador e de sua localização. Então, se o marcador possui um tamanho de três bytes e é instalado no início do bloco de marcação, o valor de marcação codificado também terá o tamanho de três bytes e será tomado no início do bloco de marcação codificado. Entretanto, é claro que, usualmente, o valor de marcação codificado MK1 não correspondente ao marcador Mc, ao qual a primeira chave de codificação K1 é aplicada. Em uma maneira similar, o elemento de enchimento codificado PADK1 não corresponde ao primeiro valor de enchimento PAD, ao qual a primeira chave de codificação K1 é aplicada.

A parte funcional PL1 contida no primeiro pacote de dados é codificada por meio de uma primeira chave de codificação K1, utilizando também, por exemplo, o método de codificação do bloco, a fim de obter a parte funcional codificada PL1K1.

O marcador Mc do pacote original DP é substituído pelo valor de marcação codificado MK1 obtido na etapa anterior. Da mesma forma, a parte funcional PL1 é substituída pela parte funcional codificada PL1K1. Este novo bloco necessariamente possui o tamanho do bloco original. Ele é chamado de bloco de dados codificado DBC. É evidente que o bloco de

dados codificado não correspondente usualmente ao pacote de dados DP, ao qual a primeira chave de codificação K1 poderia ter sido aplicada.

Outro bloco também é formado, chamado de bloco de decodificação DB, compreendendo pelo menos a primeira chave K1 e o elemento de enchimento codificado PADK1.

O bloco de dados codificado DBC e o bloco de decodificação DB são processados convencionalmente por sua difusão, quer dizer que o bloco de decodificação é geralmente codificado por uma chave de transmissão TK e formatado, a fim de ser enviado em uma mensagem de controle ECM aos receptores concernentes. O bloco de dados codificado também é transmitido a estes receptores.

Como indicado anteriormente, o método da invenção garante que uma chave que tenha servido para a codificação dos pacotes de dados nunca possa ser confundida com uma outra chave que tenha servido para outro pacote de dados.

As figuras 2 e 3 ilustram duas maneiras de assegurar que a confusão das chaves seja impossível.

Com referência a figura 2, supõe-se que os pacotes de dados anteriores tenham sido codificados por meio de uma primeira chave de codificação K1 e os pacotes seguintes são codificados por meio da chave K2.

Como indicado com referência as figuras 1a a 1g e, em particular, a figura 1b, no momento da preparação dos dados para sua transmissão, um valor de enchimento PAD1 é escolhido para formar um bloco de marcação BM, compreendendo o marcador Mc e o valor de enchimento PAD1.

Então, o bloco de marcação é codificado com uma primeira chave de codificação K1. Um bloco de marcação codificado BMC é obtido. Este é então separado em dois blocos, um contendo o valor de marcação codificado MK1 e o outro o elemento de

enchimento codificado PADK1, como demonstrado na figura 1d. Este elemento de enchimento codificado PADK1 é armazenado de forma que, no momento da etapa de verificação, ele não é recalculado, mas simplesmente extraído da memória.

Durante esta etapa de verificação, o marcador Mc ao pacote de dados é extraído. Então, um segundo valor de enchimento PAD2 é adicionado a este marcador formando um bloco de marcação possuindo o tamanho do pacote de dados. Este bloco de marcação é codificado com a segunda chave de codificação K2, formando um bloco de marcação codificado. Este último é cortado de tal maneira para formar um segundo valor de marcação codificado MK2 e um segundo elemento de enchimento codificado PADK2. O segundo valor de marcação codificado MK2 tem o tamanho do marcador e o segundo elemento de enchimento codificado PADK2 representa o equilíbrio do bloco.

Então um novo bloco é formado, chamado de bloco de marcação misto codificado BMXC, do segundo valor de marcação codificado MK2 e o primeiro elemento de enchimento codificado PADK1. Como indicado anteriormente, este primeiro elemento de enchimento codificado já é sabido, uma vez que ele foi formado durante uma etapa anterior.

Este bloco de marcação misto codificado é decodificado com uma chave utilizada anteriormente, ou seja, a primeira chave de codificação K1. O bloco obtido é cortado para formar uma primeira parte MK* possuindo a extensão do marcador e uma segunda parte PADK* representando o equilíbrio do bloco. Esta primeira parte é comparada com o marcador Mc. Se a comparação indicar que estes valores são diferentes, o método continua como explicado com referência as figuras 1a a 1g.

Do contrário, se a comparação indicar que os valores MK*, Mc são idênticos, isto pode ocorrer aleatoriamente e pode causar problemas no momento da utilização do sistema. É necessário mudar, pelo menos, um parâmetro utilizado para a codificação.

Durante o uso de um algoritmo de codificação em bloco em um método, tal como aquele descrito acima, os parâmetros utilizados são o segundo valor de enchimento PAD2, a segunda chave de codificação K2, bem como talvez um vetor de inicialização. Este

último é bem conhecido e não está descrito abaixo em detalhes. Sua função é, em particular, explicada em "Criptografia Aplicada", por Bruce Schneier, 2ª edição, §9.3.

Quando o parâmetro modificado é o valor de enchimento, este segundo valor de enchimento PAD2 será substituído por um novo segundo valor de enchimento chamado PAD2*. Se os valores de enchimento são determinados aleatoriamente, nenhum problema será causado. Se eles forem escolhidos de uma lista, é suficiente para tomar outro elemento da lista. Se o valor de enchimento é fixado, é necessário para estes casos em particular tomar um valor de enchimento diferente deste valor fixado. Por isto, é necessário providenciar os mecanismos que permitam a mudança do valor de enchimento, até mesmo se estes valores são geralmente fixados.

Quando um segundo valor de enchimento for determinado, é testado novamente até que uma configuração seja alcança, na qual o valor de marcação decodificado MK* é diferente do marcador Mc.

De acordo com uma alternativa, também é possível manter o mesmo valor de enchimento e mudar a chave. Na verdade, é necessário mudar, pelo menos, um dos valores dos parâmetros acima mencionados. Também é possível mudar todos os valores, por exemplo, por extrair aleatoriamente um novo conjunto de parâmetros utilizados, especialmente um segundo valor de enchimento, uma segunda chave e um vetor de inicialização.

De acordo com uma alternativa, mostrada na figura 3, o marcador não é testado, mas especialmente outra referência de dados é testada. Ao invés de usar o segundo valor de enchimento PAD2, tal como definido nesta figura 2, um segundo valor fixado F2 também é utilizado, de forma que o marcador Mc, o valor de enchimento PAD2 e o valor fixado F2 possuem uma extensão igual ao tamanho codificado.

O método de verificação é executado como indicado na modalidade anterior até a obtenção do bloco de marcação misto decodificado por uma primeira chave de codificação K1. Este bloco de marcação misto decodificado é cortado em três partes, especialmente a primeira parte MK* do tamanho do marcador, uma parte intermediária PADK* e uma terceira

parte FK* do tamanho do valor fixado F2. Por conhecer o primeiro valor de enchimento PAD1, o primeiro valor fixado F1 e a primeira chave de codificação K1, é possível determinar o valor que deve ser obtido para a terceira parte FK* do bloco de marcação misto decodificado, este valor sendo chamado de valor de referência previsível PDV2. Nesta modalidade, se a terceira parte FK* é igual ao valor de referência previsível PDV2, o segundo valor fixado F2, ou a chave, ou um vetor de inicialização é mudado, até a comparação indicar uma diferença nos valores.

Esta modalidade indica que não é necessário executar a comparação sobre um valor idêntico para todos os pacotes de dados. Na verdade, é suficiente aplicar este método a valores conhecidos no espaço livre, o processamento, do qual se dá um resultado previsível.

As figuras 4a a 4g descrevem a decodificação do pacote de dados DP por meio da chave K1 que tem servido para cifrar este pacote.

Como indicado com referência às figuras 1f e 1g, o receptor/decodificador recebe de um lado o bloco de dados codificado DBC e de outro lado o bloco de decodificação DB, O último sendo codificado pela chave de transmissão TK.

Em primeiro lugar, o decodificador utiliza a chave de transmissão TK para extrair o bloco de decodificação. A partir do valor de marcação codificado MK1 e o elemento de enchimento codificado PADK1, o bloco de marcação codificado BMC é reconstituído. Graças ao conhecimento da primeira chave K1, originada do bloco de decodificação, é possível decodificar o bloco de marcação codificado e obter o bloco de marcação.

Este bloco de marcação é então cortado, a fim de obter um bloco possuindo a extensão do marcador Mc. Este bloco é testado para verificar se é igual ao marcador Mc ou não.

Baseado na hipótese de que a primeira chave K1 para codificação é também utilizada para decodificação, o bloco obtido anteriormente poderia também conter o marcador Mc. Esta característica, na verdade, permite assegurar que a chave de decodificação seja também válida para o pacote de dados processado no momento.

Graças a este marcador Mc, o pacote original pode ser reconstituído por substituir o valor de marcação codificado MK1 no bloco de marcação codificado com o marcador Mc. Desta forma o pacote de dados original DP, cuja parte funcional PL1K1 que está codificada é obtido. Este é então decodificado por meio da primeira chave K1, a fim de obter a parte funcional PL1, a qual é então processada convencionalmente para acessar o conteúdo requerido.

O restante da decodificação relaciona-se ao caso onde a chave de codificação utilizada é uma segunda chave de codificação K2 e onde a primeira chave de codificação é utilizada para tentar o acesso aos dados. Este caso é considerado abaixo com referência às figuras 5a a 5d.

Como indicado anteriormente, o decodificador recebe um bloco de dados codificado DBC e um bloco de decodificação DB. Este bloco de decodificação sendo ele mesmo codificado por uma chave de transmissão TK. Este bloco é primeiro decodificado graças ao conhecimento da chave de transmissão do decodificador. O decodificador pode então formar, como na figura 4b, um bloco de marcação codificado, compreendendo o valor de marcação codificado MK2 e o elemento de enchimento codificado PADK1.

Este decodificador decifra este bloco com esta chave atual, ou seja, a primeira chave de codificação K1. O resultado é cortado à extensão do marcador Mc, e então comparado a este marcador. Como a chave K2 utilizada para a codificação é diferente da primeira chave K1 utilizada para a decodificação, a parte cortada MK2 do bloco será diferente do marcador Mc.

Ademais, como indicado com referência a figura 2, o valor de enchimento PAD1 é escolhido e verificado de tal forma que é impossível para a parte cortada do bloco ser igual ao marcador.

Deste modo, a mudança da chave será inevitavelmente detectada pelo decodificador. Como a utilização da primeira chave K1 não fornece o resultado esperado, ou

seja, o marcador Mc, a chave seguinte é utilizada, especialmente a segunda chave de codificação K2. Desta maneira, um encontra a si próprio no mesmo caso como revelado nas figuras 4a a 4g, por substituir a primeira chave de codificação K1 pela segunda chave de codificação K2, a qual permite ao marcador ser encontrado e, deste modo, acessar a parte funcional PL. Pode ser notado que, se o uso desta nova chave não der tampouco o resultado esperado, quer dizer o marcador, uma mensagem de erro será gerada.

Na descrição acima, é indicado que o atual dispositivo de decodificação contém duas chaves, ou seja, uma chave atual e uma chave seguinte. De acordo com uma alternativa, poderia conter mais, por exemplo, 5, registradas em um registro de deslocamento. Neste caso, quando uma primeira chave não é mais usável, é eliminada e a segunda chave toma seu lugar. A 5.ª chave toma o lugar da 4.ª chave e uma nova chave é introduzida na posição da 5.ª.

As chaves utilizadas na presente invenção podem ser do tipo simétrico ou assimétrico. No caso da chave simétrica, a mesma chave é utilizada para codificar, bem como para decodificar. No caso da chave assimétrica, a chave é utilizada para codificar dados é diferente da chave que permite que sejam decodificados. Então, na descrição acima, quando é indicado que a decodificação é executada com a primeira chave K1, por exemplo, é necessário entender que no caso de utilizar chaves assimétricas, esta decodificação é executada com a chave do par de chaves, o qual não tenha sido utilizado para a codificação.

Embora não seja representado explicitamente nos desenhos, quando o vetor de inicialização é utilizado no campo da codificação de bloco, este vetor é também transmitido ao decodificador no bloco de decodificação, de forma que este vetor seja também disponível durante a decodificação.

REIVINDICAÇÕES

1. Método de codificação e decodificação para conteúdo de acesso condicional, no qual referido conteúdo é transmitido na forma de pacotes de dados (DP), sendo os pacotes anteriores codificados por uma primeira chave (K1) associada a um primeiro valor de enchimento (PAD1) e a um primeiro elemento de enchimento codificado (PADK1) e os pacotes seguintes sendo codificados por uma segunda chave (K2) associada a um segundo valor de enchimento (PAD2) e a um segundo elemento de enchimento codificado (PADK2), no qual ao menos a primeira chave (K1) e o primeiro valor de enchimento (PAD1) formam um primeiro conjunto de parâmetros de codificação e, no qual, pelo menos a segunda chave (K2) e o segundo valor de enchimento formam um segundo conjunto de parâmetros de codificação. Este método compreende as seguintes etapas:

a) extração de um marcador (Mc) de um pacote de dados (DP):

b) criação de um primeiro bloco de marcação, incluindo, de um lado o marcador (Mc) e, de outro lado o segundo valor de enchimento (PAD2):

c) codificação do primeiro bloco de marcação com a segunda chave de codificação (K2):

d) extração de um segundo valor de marcação codificado (MK2) do primeiro bloco de marcação codificado:

e) criação de um bloco de marcação misto incluindo de um lado o segundo valor de marcação (MK2) e, de outro lado o primeiro valor de enchimento (PADK1):

f) decodificação do bloco de marcação por meio da primeira chave de codificação (K1), a fim de obter um bloco de marcação misto decodificado:

g) extração de uma parte predeterminada de um bloco de marcação misto decodificado:

h) comparação desta parte extraída com um valor de referência (Mc; PDV2);

i) se a comparação levar a uma igualdade, determinação de um novo conjunto de parâmetros de codificação diferente do primeiro conjunto de parâmetros de codificação e repetição das etapas b) a h), nas quais o segundo conjunto de parâmetros de codificação é substituído por um novo segundo conjunto de parâmetros de codificação.

2. Método de acordo com a reivindicação1, caracterizado pelo fato de o conjunto de parâmetros de codificação também incluir um vetor de inicialização.

3. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de referido novo conjunto de parâmetros de codificação ser diferente do primeiro conjunto de parâmetros de codificação por, pelo menos, um dos referidos parâmetros.

4. Método de acordo com a reivindicação 1, caracterizado pelo fato de durante a etapa h), a comparação da parte extraída ser feita em relação ao marcador (Mc).

5. Método de acordo com a reivindicação 1, caracterizado pelo fato de durante a etapa h), a comparação da parte extraída ser feita em relação ao valor conhecido igual a uma parte extraída do segundo valor de enchimento (PAD2).

6. Método de acordo com a reivindicação1, caracterizado pelo fato de o tamanho do bloco de marcação formado a partir do marcador (Mc) e primeiro ou segundo valor de enchimento (PAD1; PAD2) ser igual a um tamanho compatível com um algoritmo de codificação em bloco usado neste método.

7. Método de acordo com a reivindicação1, caracterizado pelo fato de a parte (MK1) do bloco de marcação misto decodificado extraída deste bloco ter um tamanho igual ao do marcador (Mc).

8. Método de acordo com a reivindicação 1, caracterizado pelo fato de também incluir as seguintes etapas:

- criação de um primeiro bloco de marcação incluindo de um lado o marcador (Mc) e do outro um primeiro valor de enchimento (PAD1);

- codificação do bloco de marcação com a primeira chave (K1);

- extração de um primeiro valor de marcação codificado (MK1) do bloco de marcação codificado;

- substituição em um pacote de dados (DP) do marcador (Mc) com a parte (MK1) do bloco de marcação codificado extraído deste bloco, esta parte sendo chamada de valor de marcação codificado, o resultado desta substituição sendo chamado de bloco de dados codificado;

- criação de um bloco de decodificação formado, pelo menos, de um lado por uma primeira chave de codificação (K1) e de outro lado por um elemento de enchimento codificado (PADK1), sendo este formado pelo bloco de marcação codificado, do qual tenha sido retirado o valor de marcação codificado (MK1).

9. Método de acordo com a reivindicação 8, caracterizado pelo fato do bloco de dados codificado e o bloco de decodificação serem transmitidos, pelo menos a um receptor, dito bloco de decodificação também sendo codificado por uma chave de transmissão (TK).

10. Método de decodificação de acordo com a reivindicação 9, caracterizado pelo fato de incluir as seguintes etapas:

a) recepção do bloco de dados codificado e do bloco de decodificação e, decodificação do bloco de decodificação por meio da chave de transmissão (TK);
b) criação do bloco de marcação codificado por extração do valor de marcação codificado (MK1) originado do bloco de dados codificado e por extração do elemento de enchimento codificado (PADK1) originado do bloco de decodificação;

c) decodificação do bloco de marcação codificado por meio de uma chave atual (K1);

d) extração de uma parte predeterminada de um bloco de marcação obtida durante a decodificação do bloco de marcação codificado;

e) comparação desta parte predeterminada do bloco de marcação com um valor de referencia (Mc: PDV2);

f) no caso de igualdade, substituição do valor de marcação codificado (MK1) do bloco de dados codificado com referido marcador (Mc);

g) extração, decodificação e uso da parte funcional (PL);

h) no caso de não haver igualdade no momento da comparação, decodificação ou codificação do bloco de marcação por meio de uma chave seguinte (K2);

i) extração de uma parte predeterminada de um bloco de marcação obtida durante a decodificação do bloco de marcação com esta nova chave (K2);

j) comparação desta parte do bloco de marcação com o valor de referencia (Mc: PDV2);

k) no caso de igualdade, substituição do valor de marcação codificado (MK1) do bloco de dados codificado por dito marcador (Mc);

l) extração, decodificação e uso da parte funcional (PL).

11. Método de acordo com a reivindicação 10, caracterizado pelo fato de no caso de não haver igualdade após a decodificação com a chave seguinte (K2), geração de uma mensagem de erro.

12. Método de acordo com a reivindicação 10, caracterizado pelo fato de a comparação da parte predeterminada extraída ser feita em relação ao marcador (Mc).

13. Método de acordo com a reivindicação 10, caracterizado pelo fato de a comparação da parte predeterminada extraída ser feita em comparação com o valor sabido igual a uma parte extraída do primeiro valor de enchimento (PADI).

14. Método de acordo com a reivindicação 11, caracterizado pelo fato de o tamanho do bloco extraído do bloco de marcação codificado ser igual ao tamanho do marcador (Mc).

15. Método de acordo com a reivindicação 1, caracterizado pelo fato de duas chaves serem armazenadas, uma tendo a função da chave atual e a outra tendo a função de chave seguinte.

16. Método de acordo com a reivindicação 1, caracterizado pelo fato de várias chaves serem armazenadas e associadas a uma ordem de uso.

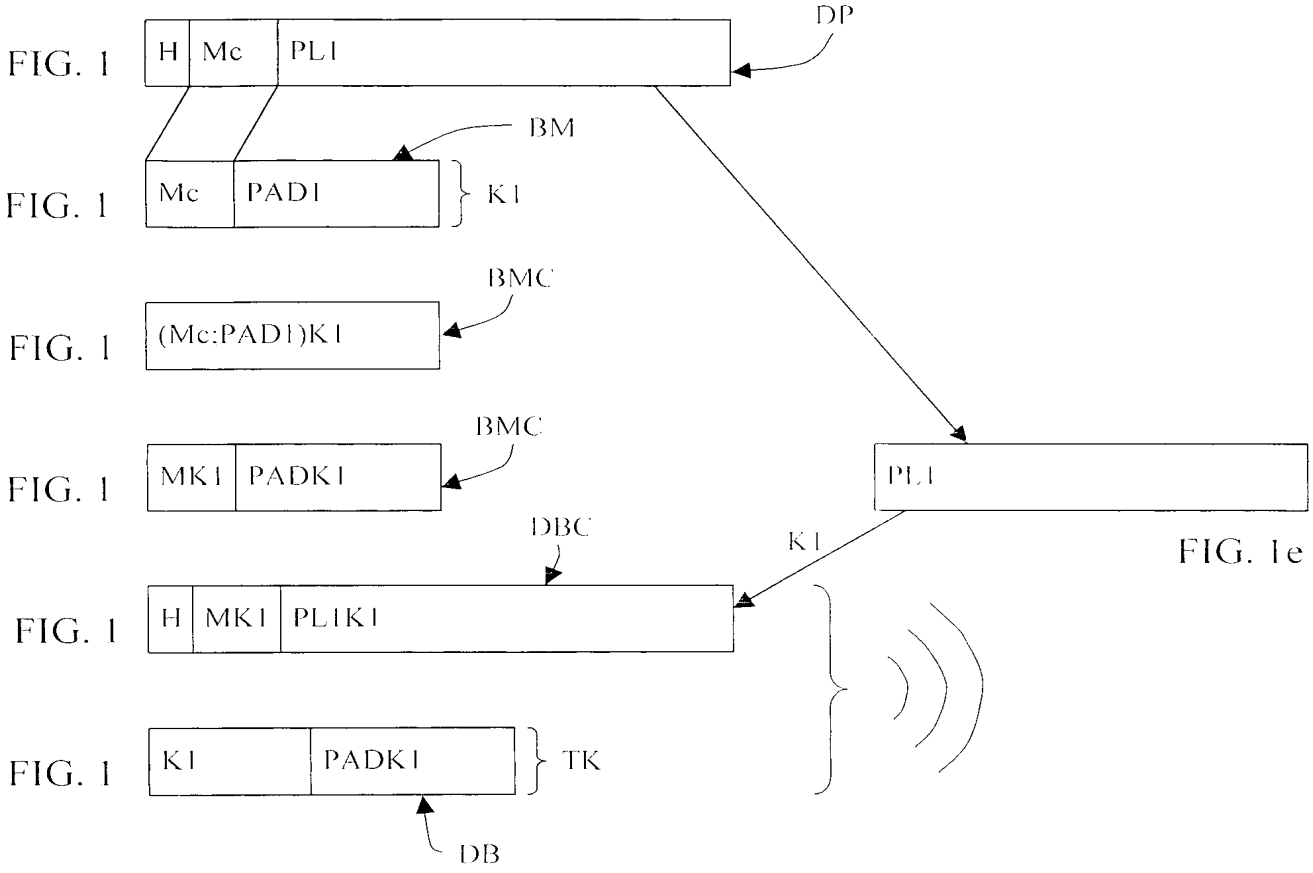


FIG. 1
H
Mc
PL1
DP
FIG. 1
Mc
PAD1
BM
K1
FIG. 1
(Mc:PAD1)K1
BMC
FIG. 1
MK1
PADK1
BMC
PL1
FIG. 1e
K1
DBC
FIG. 1
H
MK1
PL1K1
FIG. 1
K1
PADK1
TK
DB

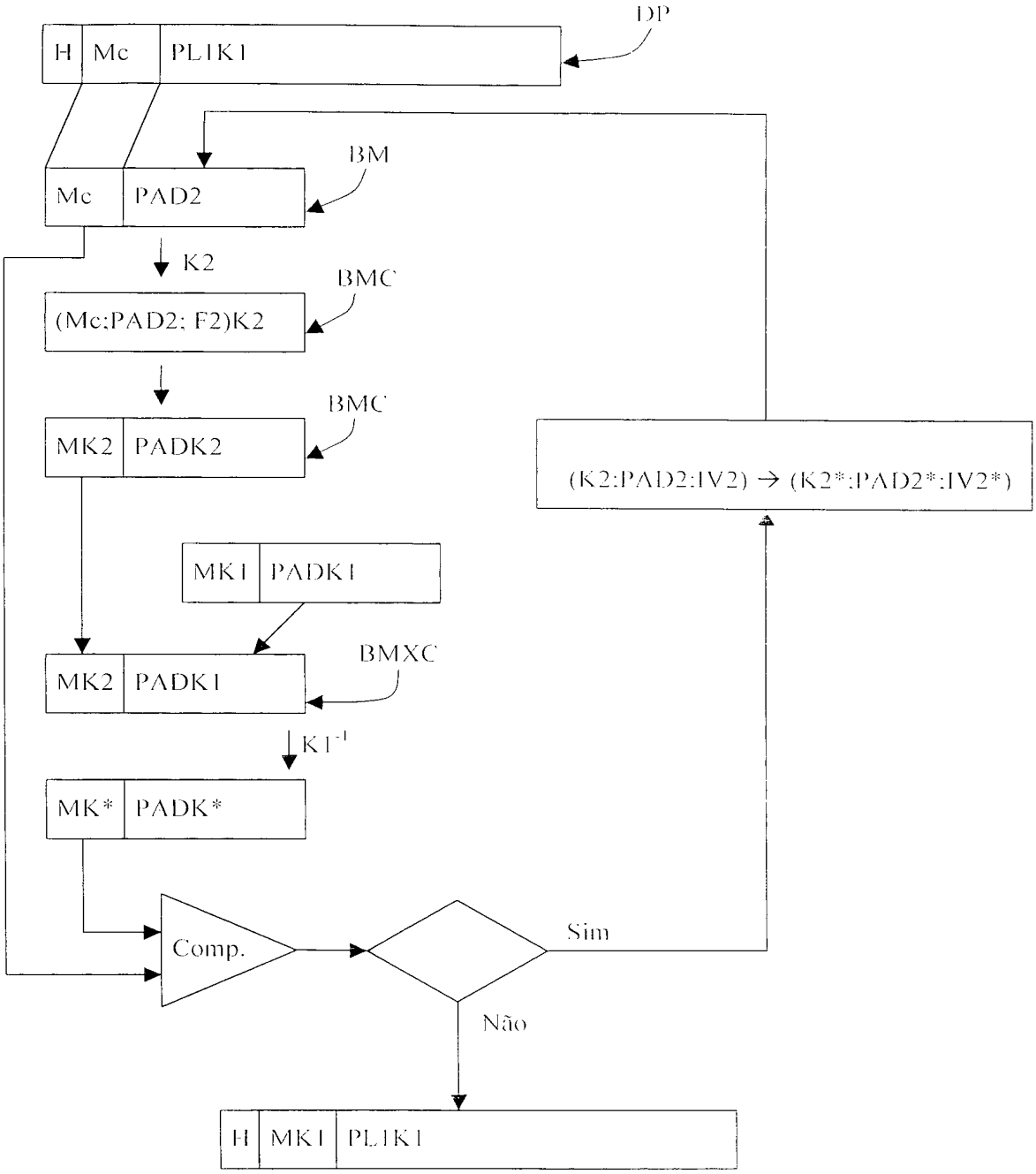

DP
H
Mc
PL1K1
BM
Mc
PAD2
K2
BMC
(Mc;PAD2; F2)K2
BMC
MK2
PADK2
(K2:PAD2:IV2) → (K2*:PAD2*:IV2*)
MK1
PADK1
BMXC
MK2
PADK1
K1-1
MK*
PADK*
Comp.
Sim
Não
H
MK1
PL1K1

FIG.

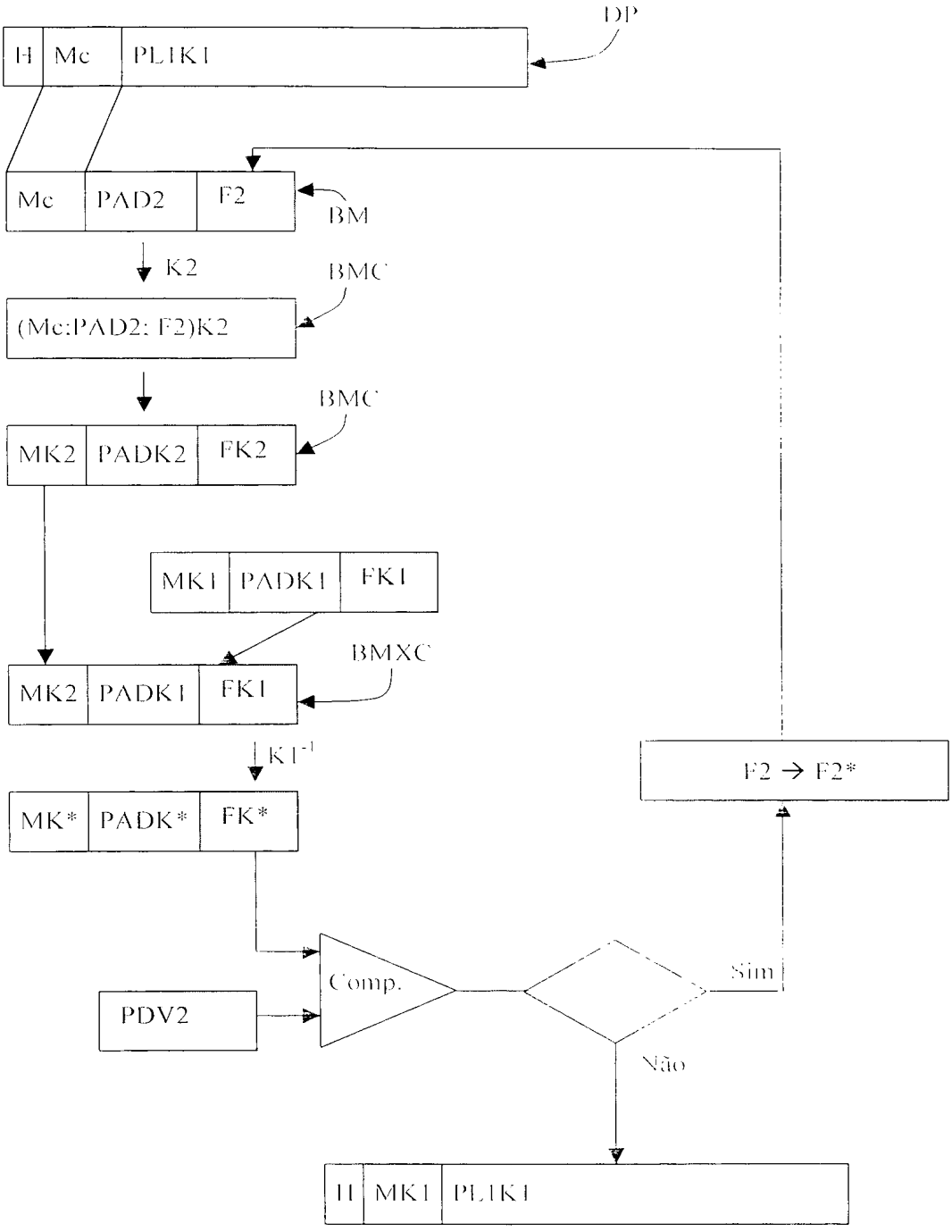
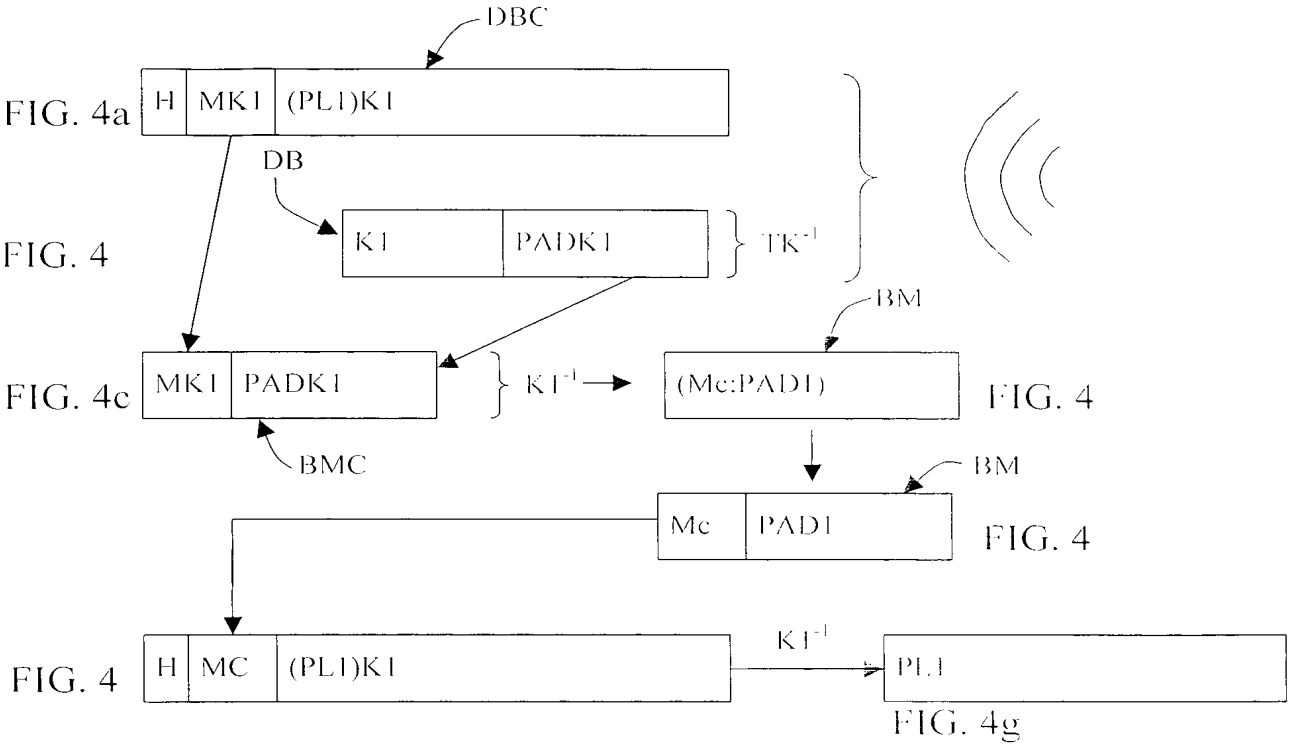
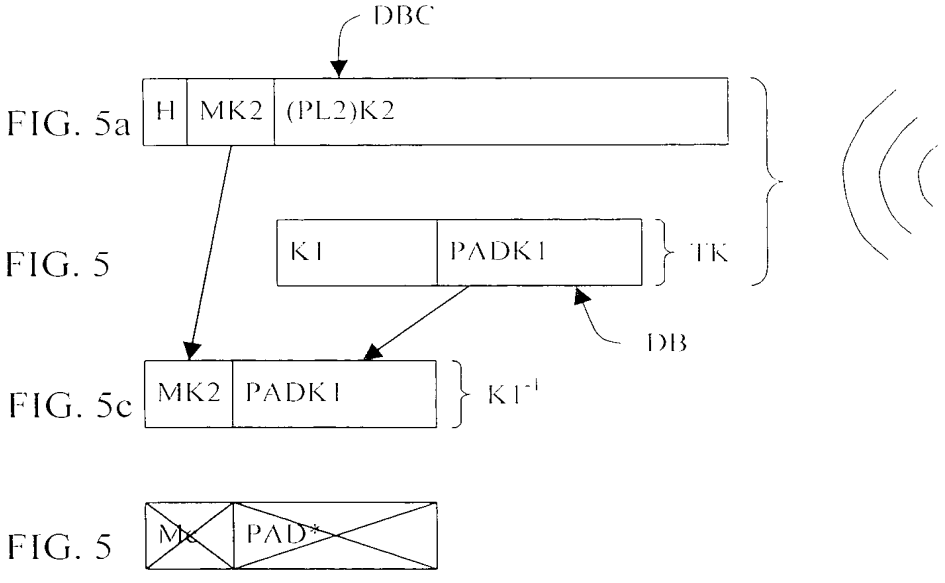

DP
H
Mc
PL1K1
Mc
PAD2
F2
BM
K2
BMC
(Mc:PAD2: F2)K2
BMC
MK2
PADK2
FK2
MK1
PADK1
FK1
BMXC
MK2
PADK1
FK1
K1-1
MK*
PADK*
FK*
F2 → F2*
Comp.
PDV2
Sim
Não
H
MK1
PL1K1

FIG. 3


DBC
H
MK1
(PL1)K1
FIG. 4a
DB
K1
PADK1
TK-1
FIG. 4
BM
MK1
PADK1
K1-1
(Mc:PAD1)
FIG. 4
FIG. 4c
BMC
BM
Mc
PAD1
FIG. 4
H
MC
(PL1)K1
K1-1
PL1
FIG. 4
FIG. 4g


DBC
H
MK2
(PL2)K2
FIG. 5a
K1
PADK1
TK
FIG. 5
DB
MK2
PADK1
K1-1
FIG. 5c
Mc
PAD*
FIG. 5

RESUMO

Esta invenção é relativa ao método de codificação e decodificação para u conteúdo de acesso condicional, no qual o conteúdo é transmitido na forma de pacotes de dados (DP), os pacotes anteriores sendo codificados por uma primeira chave (K1) associada a um primeiro valor de enchimento (PAD1) e a um primeiro elemento de enchimento codificado (PADK1) e os pacotes seguintes sendo codificados por uma segunda chave (K2) associada a um segundo valor de enchimento (PAD2) e a um segundo elemento de enchimento codificado (PADK2). Neste método, a primeira chave (K1) e o primeiro valor de enchimento (PAD1) formam um primeiro conjunto de parâmetros de codificação, a segunda chave (K2) e o segundo valor de enchimento formando um segundo conjunto de parâmetros de codificação. Este método inclui as etapas de (a) extração de marcador (Mc) de um pacote de dados (DP);(b) criação de um primeiro bloco de marcação incluindo um marcador (Mc) e o segundo valor de enchimento (PAD2); (c) codificação do primeiro bloco de marcação com a segunda chave de codificação (K2); (d) extração de um segundo valor de marcação codificado (MK2) do primeiro bloco de marcação codificado; (e) criação de um bloco de marcação misto incluindo um segundo valor de marcação codificado (MK2) e um primeiro elemento de enchimento codificado (PADK1); (f) decodificação do bloco de marcação misto por meio da primeira chave de codificação (K1), a fim de obter um bloco de marcação misto decodificado; (g) extração de uma parte predeterminada do bloco de marcação misto decodificado; (h) comparação desta parte extraída com um valor de referência (Mc; PDV2); (i) se a comparação levar a igualdade, determinação de uma novo conjunto de parâmetros de codificação diferente do primeiro conjunto de parâmetros de codificação e repetição das etapas b) a h), nas quais o segundo conjunto de parâmetros de codificação é substituído pelo novo segundo conjunto de parâmetros de codificação.