(11) Número de Publicação: **PT 2273818 E**

(51) Classificação Internacional:
H04W 36/08 (2011.01) *H04W 12/04* (2011.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2009.06.17**

(30) Prioridade(s): **2008.06.23 CN 200810067995**

(43) Data de publicação do pedido: **2011.01.12**

(45) Data e BPI da concessão: **2012.03.14 103/2012**

(73) Titular(es):
HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI ADMINISTRATION BUILDING BANTIAN LONGGANG DISTRICT, SHENZHEN GUANGDONG 518129 **CN**

(72) Inventor(es):
MIN HUANG **CN**
JING CHEN **CN**
AIQIN ZHANG **CN**
XIAOHAN LIU **CN**

(74) Mandatário:
MARIA SILVINA VIEIRA PEREIRA FERREIRA
RUA CASTILHO, N.º 50, 5º - ANDAR 1269-163 LISBOA **PT**

(54) Epígrafe: **MÉTODO, APARELHO E SISTEMA DE DERIVAÇÃO DE CHAVES**

(57) Resumo:
SÃO DIVULGADOS UM MÉTODO, APARELHO E SISTEMA PARA DERIVAÇÃO DE CHAVES. O MÉTODO INCLUI AS SEGUINTES FASES: UMA ESTAÇÃO DE BASE DE DESTINO RECEBE MÚLTIPLAS CHAVES DERIVADAS DE UMA ESTAÇÃO DE BASE DE ORIGEM, EM QUE AS CHAVES CORRESPONDEM A MÚLTIPLAS CÉLULAS SOB CONTROLO DA ESTAÇÃO DE BASE DE DESTINO; A ESTAÇÃO DE BASE DE DESTINO SELECIONA UMA CHAVE CORRESPONDENTE À CÉLULA DE DESTINO DEPOIS DE SABER UMA CÉLULA DE DESTINO À QUAL UM EQUIPAMENTO DE UTILIZADOR (UE) PRETENDE ACEDER. UM APARELHO PARA DERIVAÇÃO DE CHAVES E UM SISTEMA DE COMUNICAÇÃO SÃO IGUALMENTE FORNECIDOS.

RESUMO

"MÉTODO, APARELHO E SISTEMA DE DERIVAÇÃO DE CHAVES"

São divulgados um método, aparelho e sistema para derivação de chaves. O método inclui as seguintes fases: uma estação de base de destino recebe múltiplas chaves derivadas de uma estação de base de origem, em que as chaves correspondem a múltiplas células sob controlo da estação de base de destino; a estação de base de destino seleciona uma chave correspondente à célula de destino depois de saber uma célula de destino à qual um equipamento de utilizador (UE) pretende aceder. Um aparelho para derivação de chaves e um sistema de comunicação são igualmente fornecidos.

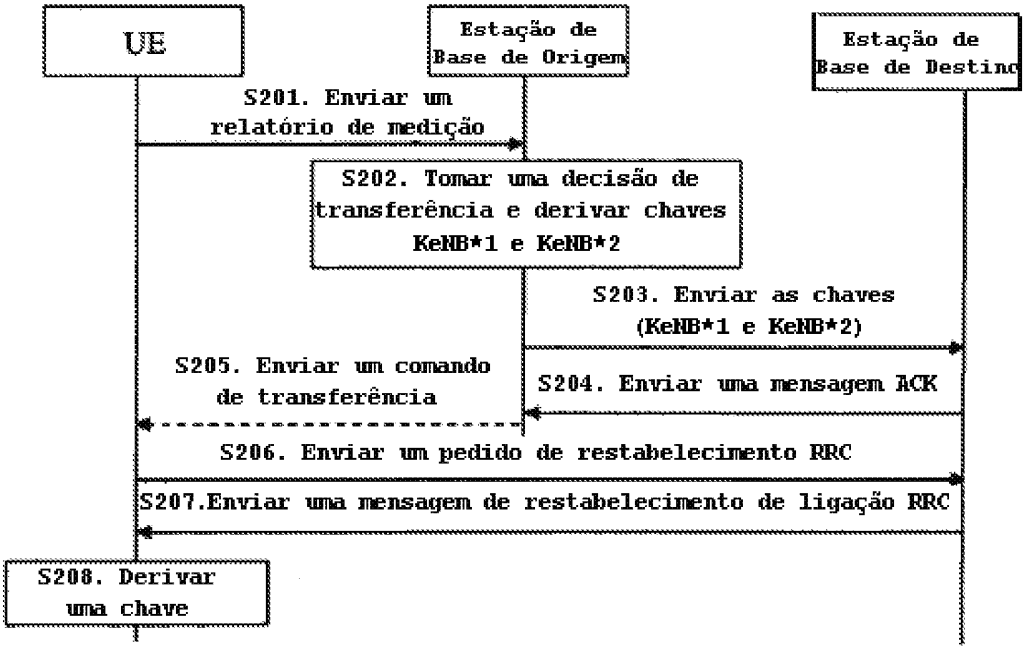

FIG. 2

DESCRIÇÃO
"MÉTODO, APARELHO E SISTEMA DE DERIVAÇÃO DE CHAVES"

Campo da Invenção

A presente invenção refere-se ao campo da comunicação móvel e, em particular, a um método, um aparelho e um sistema para derivação de chaves.

Antecedentes da Invenção

Num sistema de evolução a longo prazo (LTE) do estado da técnica, se um equipamento de utilizador (UE) em estado de ligação detetar que a qualidade de sinal numa célula de origem é fraca, a estação de base da célula de origem (a seguir referida como estação de base de origem) efetua as seguintes preparações de transferência depois de receber um relatório de medição do UE. A estação de base de origem deriva uma chave A de acordo com um identificador (ID) de célula física da célula de destino, envia a chave A para a estação de base X de uma célula de destino A (a seguir referida como estação de base de destino), e envia um comando de transferência para o UE. Se o UE não puder receber o comando de transferência em caso de falha de ligação via rádio (RLF - Radio Link Failure), o UE volta a selecionar uma célula apropriada e inicia um procedimento de restabelecimento de ligação de controlo de recurso de rádio (RRC - Radio Resource Control) para retomar o serviço.

Na solução técnica do estado da técnica, quando a estação de base de uma célula de destino B à qual o UE tenta aceder através do procedimento de restabelecimento de ligação é a mesma estação de base da célula de destino A, o UE deriva

uma chave B utilizando o ID de célula física da célula de destino B, e encripta mensagens enviadas pelo UE à estação de base X utilizando a chave B; a estação de base X desencripta as mensagens enviadas pelo UE utilizando a chave A de acordo com as informações de contexto do UE. Deste modo, as chaves utilizadas pelo UE e a estação de base X são inconsistentes, o que conduz a uma falha de comunicação entre o UE e a estação de base.

O documento *3GPP TS 33.abc V1.0.0 (2008-02)* divulga a arquitetura de segurança, ou seja, as funcionalidades de segurança e os mecanismos de segurança para o sistema de pacotes de tecnologia avançada e o núcleo de pacotes de tecnologia avançada, e os procedimentos de segurança efetuados no sistema de pacotes de tecnologia avançada (EPS) incluindo o núcleo de pacotes de tecnologia avançada (EPC) e o UTRAN de tecnologia avançada (E-UTRAN).

Resumo da Invenção

A presente invenção fornece um método, um aparelho e um sistema para derivação de chaves para resolver a falha de comunicação entre um UE que tenta aceder a uma célula de destino.

De acordo com um aspeto da presente invenção, é fornecido um método para derivação de chaves, que inclui:

a receção, através de uma estação de base de destino, de múltiplas chaves derivadas de uma estação de base de origem, em que as múltiplas chaves correspondem a múltiplas células sob controlo da estação de base de destino;
a receção, através da estação de base de destino, de um pedido de restabelecimento de ligação de controlo de

recurso de rádio (RRC) de um Equipamento de Utilizador (UE); e

a seleção, através da estação de base de destino, de uma chave a partir das múltiplas chaves recebidas pela estação de base de destino para ser utilizada na comunicação com o UE, sendo que a chave selecionada corresponde à célula de destino à qual o UE pede para aceder durante o procedimento de restabelecimento de ligação.

De acordo com outro aspeto da presente invenção, é fornecido um aparelho numa estação de base que funciona como uma estação de base de destino para um Equipamento de Utilizador (UE), que inclui:

uma primeira unidade configurada para receber múltiplas chaves derivadas de uma estação de base de origem, sendo que as múltiplas chaves correspondem a múltiplas células sob controlo de uma estação de base de destino, em que a primeira unidade é ainda configurada para receber uma mensagem de pedido de restabelecimento de ligação de Controlo de Recurso de Rádio (RRC) de um Equipamento de Utilizador (UE); e

uma segunda unidade configurada para selecionar uma chave a partir das múltiplas chaves recebidas pela estação de base de destino para ser utilizada na comunicação com o UE, sendo que a chave selecionada corresponde à célula de destino à qual o UE pede para aceder durante o procedimento de restabelecimento de ligação.

De acordo com outro aspeto da presente invenção, é fornecido um aparelho numa estação de base que funciona

como uma estação de base de origem para um Equipamento de Utilizador (UE), que inclui: meios para derivar múltiplas chaves que correspondem a múltiplas células sob controlo de uma estação de base de destino; e meios para enviar as múltiplas chaves para a estação de base de destino.

De acordo com ainda outro aspeto da presente invenção, um sistema de comunicações inclui o aparelho da presente invenção e o UE que comunica com o aparelho.

Na presente invenção, o UE e o aparelho de rede derivam chaves utilizando os mesmos parâmetros de derivação de chaves. Deste modo, o UE e o aparelho de rede derivam a mesma chave, o que garante uma comunicação normal entre o UE e o aparelho de rede, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

Descrição Breve das Figuras

A FIG. 1 é um fluxograma de um método para derivação de chaves que não divulga todas as funcionalidades necessárias para implementar a presente invenção.

A FIG. 2 é um fluxograma de um método para derivação de chaves de acordo com uma forma de realização exemplar da presente invenção.

A FIG. 3 é um fluxograma de um método para derivação de chaves que não divulga todas as funcionalidades necessárias para implementar a presente invenção.

A FIG. 4 é um diagrama esquemático que ilustra um aparelho para derivação de chaves que não divulga todas as

funcionalidades necessárias para implementar a presente invenção.

A FIG. 5 é um diagrama esquemático que ilustra um aparelho para derivação de chaves de acordo com outra forma de realização exemplar da presente invenção.

A FIG. 6 é um diagrama esquemático que ilustra um aparelho para derivação de chaves de acordo com outra forma de realização exemplar da presente invenção.

A FIG. 7 é um diagrama esquemático que ilustra um sistema de comunicações de acordo com outra forma de realização exemplar da presente invenção.

Descrição Detalhada da Invenção

A solução técnica da presente invenção é a seguir descrita em detalhe relativamente às figuras em anexo. É evidente que as formas de realização são apenas exemplares e que a presente invenção não se limita a estas formas de realização.

Num exemplo do método para derivação de chaves quando a estação de base de destino recebe, pelo menos, uma chave derivada de acordo com o identificador (ID) de estação de base de destino e/ou ID de célula física (PCI - Physical Cell ID) da célula de destino, na receção de um pedido de restabelecimento de ligação RRC de um UE, a estação de base de destino seleciona uma Chave A e fornece ao UE o ID de estação de base de destino ou o ID de célula física da célula de destino necessário para derivar a Chave A. A Chave A selecionada pode ser derivada de acordo com o ID de estação de base de destino ou de acordo com o ID de célula

física da célula de destino correspondente à célula onde o UE se encontra ou de acordo com o ID de célula física incluído no pedido de restabelecimento de ligação RRC. Deste modo, a chave derivada do UE é consistente com a chave determinada pela estação de base de destino, o que garante uma comunicação normal entre o UE e a estação de base, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

Num exemplo do método para derivação de chaves, o UE inicia um procedimento de restabelecimento de ligação, e deriva uma chave de acordo com o ID de estação de base de destino ou o ID de célula física da célula de destino fornecido pela estação de base de destino. Deste modo, a chave derivada do UE é consistente com a chave utilizada pela estação de base de destino, o que garante uma comunicação normal entre o UE e o eNodeB, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

No estado da técnica, o processo de derivação de chaves inclui um processo de derivação primário, no qual uma chave KeNB* é derivada de acordo com o ID de célula física da célula de destino, e um processo secundário, no qual uma chave KeNB** é derivada de acordo com a KeNB* derivada no processo de derivação primário. O processo de derivação de chaves realizado pelo UE e o aparelho de rede nas formas de realização da presente invenção é o processo de derivação primário. No método para derivação de chaves numa forma de realização da presente invenção, o UE e o aparelho de rede derivam a mesma KeNB* no processo de derivação primário. Deste modo, o UE e o aparelho de rede derivam igualmente a mesma KeNB** no processo de derivação secundário, de modo a que o UE e o aparelho de rede possam manter comunicações

normais utilizando a KeNB**. É compreensível para os peritos na especialidade que o método para derivação de chaves descrito nas formas de realização exemplares da presente invenção possa ser combinado com o método envolvido no processo de derivação secundário do estado da técnica, cuja descrição detalhada é aqui omitida.

A FIG. 1 é um fluxograma de um método para derivação de chaves de acordo com um exemplo. Conforme ilustrado na FIG. 1, uma estação de base de origem é um aparelho de rede (por exemplo, eNode B) que serve atualmente um UE, e a estação de base de destino é outro aparelho de rede selecionado pela estação de base de origem para servir o UE. O método inclui as seguintes fases:

S101. O UE envia um relatório de medição para a estação de base de origem.

S102. A estação de base de origem toma uma decisão de transferência e deriva chaves de acordo com o ID de célula física da célula de destino obtido e o ID de estação de base de destino respetivamente.

Nesta fase, é presumido que a chave derivada de acordo com o ID de célula física da célula de destino é KeNB*1 e a chave derivada de acordo com o ID de estação de base de destino é KeNB*2.

É compreensível para os peritos na especialidade que vários métodos e algoritmos de derivação de chaves do estado da técnica sejam aplicáveis ao processo de derivação de chaves nesta fase, e não são descritos em mais pormenor.

S103. A estação de base de origem envia a KeNB*1 e a KeNB*2 para a estação de base de destino.

Nesta fase, as chaves podem ser incluídas numa mensagem de nível de acesso enviada através de uma interface X2 entre a estação de base de origem e a estação de base de destino. Por exemplo, as chaves são incluídas nos campos reservados ou campos expandidos de uma mensagem existente (por exemplo, um pedido de transferência) ou de uma mensagem nova. As chaves podem igualmente ser incluídas numa mensagem enviada por uma interface S1 entre a estação de base de origem e uma entidade de gestão de mobilidade (MME - Mobility Management Entity), e a MME fornece as chaves recebidas à estação de base de destino.

S104. A estação de base de destino armazena a chave recebida e envia uma mensagem de Confirmação (ACK - Acknowledgement) de pedido de transferência.

S105. A estação de base de origem envia um comando de transferência para o UE.

Se o UE receber o comando de transferência, o UE executa S106' (não ilustrado na Figura). Ou seja, o UE deriva uma chave KeNB*1' de acordo com o ID de célula física da célula de destino. A KeNB*1' é consistente com a KeNB*1 armazenada na estação de base de destino em termos de parâmetros e algoritmos de derivação e, por conseguinte, a KeNB*1' é consistente com a KeNB*1.

Se ocorrer uma Falha de Ligação via Rádio (RLF) ou falha de transferência, o procedimento de restabelecimento de ligação iniciado pelo UE pode incluir as seguintes fases:

S106. O UE envia um pedido de restabelecimento de ligação RRC para a estação de base de destino.

S107. Se a estação de base de destino receber o pedido de restabelecimento de ligação e descobrir que a chave correspondente ao UE está armazenada na estação de base de destino, a estação de base de destino seleciona a KeNB*2 e envia uma mensagem de restabelecimento de ligação RRC para o UE.

Nesta fase, a estação de base de destino pode procurar as informações de contexto na estação de base de destino de acordo com as informações de UE, de modo a descobrir se a chave correspondente ao UE está armazenada na estação de base de destino. O processo de seleção da KeNB*2 através da estação de base de destino é um processo de derivação secundário efetuado pela estação de base de destino de acordo com a KeNB*2. Se, depois de procurar as informações de contexto, a estação de base de destino descobrir que a chave correspondente ao UE não está armazenada na estação de base de destino, a estação de base de destino pode estabelecer uma comunicação com o UE para obter as informações de contexto do UE e selecionar algumas das informações de contexto para armazenar, o que não afeta a implementação.

S108. O UE recebe a mensagem de restabelecimento de ligação RRC e deriva uma chave KeNB*2′ de acordo com o ID de estação de base de destino obtido.

Nesta fase, a KeNB*2′ é consistente com a KeNB*2 armazenada na estação de base de destino em termos de parâmetros e

algoritmos de derivação e, por conseguinte, a KeNB*2' é consistente com a KeNB*2. A KeNB*2' derivada do UE é utilizada no processo de derivação secundário.

Nesta fase, o ID de estação de base de destino obtido pelo UE pode provir de uma mensagem de difusão do sistema. Ou seja, antes de iniciar o procedimento de restabelecimento de ligação ou depois de receber a mensagem de restabelecimento de ligação RRC, o UE lê o ID de estação de base de destino incluído na mensagem de difusão do sistema. O ID de estação de base de destino obtido pelo UE pode provir igualmente da mensagem de restabelecimento de ligação RRC. Ou seja, a mensagem de restabelecimento de ligação RRC enviada pela estação de base de destino ao UE na fase S107 inclui um ID de estação de base de destino, e o UE lê o ID de estação de base de destino e deriva uma chave na fase S108, tornando desnecessária a leitura da mensagem de difusão do sistema. Além disso, o ID de estação de base de destino obtido pelo UE pode provir de outras mensagens enviadas pela estação de base de destino ao UE.

É compreensível para os peritos na especialidade que um identificador global de célula (CGI - Cell Global Identifier) inclua informações sobre o ID de estação de base de destino. Deste modo, a mensagem que inclui o ID de estação de base de destino pode ser igualmente a mensagem que inclui o CGI. O recetor lê as informações sobre o ID de estação de base de destino a partir do CGI e, em seguida, utiliza o ID de estação de base de destino.

Neste exemplo, a estação de base de origem envia as duas chaves derivadas para a estação de base de destino. Se o UE executar a transferência com êxito, o UE comunica com a

estação de base de destino utilizando a chave derivada de acordo com o ID de célula física da célula de destino. Quando é efetuado o procedimento de restabelecimento de ligação no caso de uma RLF ou falha de transferência do UE, o UE comunica com a estação de base de destino utilizando a chave derivada de acordo com o ID de estação de base de destino. Deste modo, é garantida uma comunicação normal entre o UE e o aparelho de rede. O método fornecido nesta forma de realização pode reduzir a taxa de queda de chamadas e originar uma melhor experiência de utilizador sem alterar a interface aérea.

Outro exemplo é semelhante ao exemplo anterior, com a exceção da seguinte diferença: a estação de base de origem deriva uma chave de acordo com o ID de estação de base de destino obtido em vez do ID de célula física da célula de destino, e envia a KeNB*2 derivada para a estação de base de destino; a estação de base de destino inclui um ID de estação de base de destino no comando de transferência enviado ao UE, de modo a que o UE possa derivar a KeNB*2' de acordo com o ID de estação de base de destino depois de receber o comando de transferência. Deste modo, a KeNB*2' é consistente com a KeNB*2. Além disso, se o UE iniciar um procedimento de restabelecimento de ligação devido a uma falha ao receber o comando de transferência, a estação de base de destino inclui o ID de estação de base de destino na mensagem de restabelecimento de ligação RRC enviada ao UE ou inclui o ID de estação de base de destino na mensagem de difusão do sistema, de modo a que o UE derive a KeNB*2' de acordo com o ID de estação de base de destino lido a partir da mensagem de restabelecimento de ligação RRC ou mensagem de difusão do sistema. Deste modo, a KeNB*2' é consistente com a KeNB*2.

Neste exemplo, o UE e o aparelho de rede derivam chaves utilizando o ID de estação de base de destino como parâmetro. Deste modo, as chaves derivadas pelo UE e o aparelho de rede são consistentes, o que garante uma comunicação normal entre o UE e o aparelho de rede, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

A FIG. 2 é um fluxograma de um método para derivação de chaves de acordo com uma forma de realização exemplar da presente invenção. Conforme ilustrado na FIG. 2, a estação de base de origem é um aparelho de rede (por exemplo, eNodeB de origem) que serve atualmente o UE, e a estação de base de destino é outro aparelho de rede (por exemplo, eNode B de destino) selecionado pela estação de base de origem para servir o UE. O método inclui as seguintes fases:

S201. O UE envia um relatório de medição para a estação de base de origem.

S202. A estação de base de origem toma uma decisão de transferência, procura todos os IDs de célula física das células de destino correspondentes à estação de base de origem de acordo com o ID de estação de base de destino obtido e deriva chaves de acordo com os IDs de célula física das células de destino respetivamente.

Nesta fase, é presumido que a estação de base de destino tem três células; ou seja, existem IDs de célula física de três células de destino correspondentes ao ID de estação de base de destino, nomeadamente, Célula1, Célula2 e Célula3.

Deste modo, são derivadas três chaves representadas por KeNB*1, KeNB*2 e KeNB*3.

É compreensível para os peritos na especialidade que vários métodos e algoritmos de derivação de chaves do estado da técnica sejam aplicáveis ao processo de derivação de chaves nesta fase, e não são descritos em mais pormenor.

S203. A estação de base de origem envia a KeNB*1, a KeNB*2 e a KeNB*3 para a estação de base de destino.

Nesta fase, as chaves podem ser incluídas numa mensagem de nível de acesso enviada através da interface X2 entre a estação de base de origem e a estação de base de destino. As chaves podem ser incluídas nos campos reservados ou campos expandidos de uma mensagem existente (por exemplo, um pedido de transferência) ou de uma mensagem nova. As chaves podem ser igualmente incluídas numa mensagem enviada pela interface S1 entre a estação de base de origem e a MME, e a MME fornece as chaves recebidas à estação de base de destino. Além disso, a estação de base de origem pode incluir múltiplas chaves numa mensagem para transmissão, de modo a guardar recursos e melhorar a eficiência de transmissão. Além disso, a estação de base de origem pode incluir igualmente múltiplas chaves para mensagens diferentes para transmissão, de modo a melhorar a flexibilidade de transmissão.

S204. A estação de base de destino armazena as chaves recebidas e envia uma mensagem ACK de pedido de transferência.

S205. A estação de base de origem envia um comando de transferência para o UE.

Se o UE receber o comando de transferência e obtiver um ID de célula física da célula de destino, por exemplo Célula1, o UE executa S206' (não ilustrado na figura). Ou seja, o UE deriva uma KeNB*1' de acordo com o ID de célula física da Célula1. A KeNB*1' é consistente com a KeNB*1 da estação de base de destino em termos de parâmetros e algoritmos de derivação e, por conseguinte, a KeNB*1' é consistente com a KeNB*1.

Se o UE não puder receber o comando de transferência no caso de uma RLF, o procedimento de restabelecimento de ligação iniciado pelo UE inclui as seguintes fases:

S206. O UE envia um pedido de restabelecimento de ligação RRC para a estação de base de destino.

S207. A estação de base de destino recebe o pedido de restabelecimento de ligação e é informada de que um ID de célula física da célula à qual o UE pede para aceder é o ID de Célula2 da estação de base de destino. A estação de base de destino utiliza a KeNB*2 correspondentes à Célula2 e envia uma mensagem de restabelecimento de ligação RRC ao UE.

S208. O UE recebe a mensagem de restabelecimento de ligação RRC e deriva uma KeNB*2' de acordo com a Célula2.

Nesta fase, a KeNB*2' é consistente com a KeNB*2 armazenada na estação de base de destino em termos de parâmetros e

algoritmos de derivação e, por conseguinte, a KeNB*2' é consistente com a KeNB*2.

Nesta fase, o ID de célula física da célula de destino obtido pelo UE pode provir de um ID de camada física difundido no sistema ou da mensagem de restabelecimento de ligação RRC. A estação de base de destino pode incluir um ID de célula física da célula de destino na mensagem de restabelecimento de ligação RRC enviada ao UE na fase S207, e o UE lê o ID de célula física da célula de destino e deriva uma chave na fase S208. O ID de célula física da célula de destino obtido pelo UE pode provir igualmente de outras mensagens enviadas pela estação de base de destino ao UE.

Nesta forma de realização, a estação de base de origem envia todas as chaves derivadas de acordo com os IDs de célula física das células de destino para a estação de base de destino, de modo a que a estação de base de destino possa selecionar uma chave para ser utilizada nas comunicações com o UE de acordo com uma célula à qual o UE pretende aceder. Deste modo, a taxa de sucesso de acesso do UE a novas células aumenta e pode atingir os 100%. A estação de base de origem pode selecionar igualmente algumas chaves e enviá-las para a estação de base de destino de acordo com algumas condições; por exemplo, só pode enviar chaves derivadas de acordo com os IDs de célula física das células de destino com maior prioridade. A estação de base de origem pode derivar igualmente chaves de acordo com algumas condições; por exemplo, só pode derivar chaves de acordo com os IDs de célula física das células de destino com menor prioridade e enviar as chaves derivadas para a estação de base de destino. Deste modo, a taxa de

sucesso de acesso do UE aumenta e a quantidade de informações transmitidas através da estação de base de origem diminui, mas a taxa de sucesso de acesso do UE é inferior a 100%.

No método fornecido na forma de realização exemplar anterior da presente invenção, se ocorrer uma RLF quando o UE aceder a uma célula a1 de uma estação de base de destino A, o UE pode aceder a uma célula a2 da estação de base de destino através do procedimento de restabelecimento de ligação. Convém mencionar que o relatório de medição enviado à estação de base de origem pelo UE inclui informações de múltiplas estações de base de destino acessíveis. Deste modo, o processo de derivação de chaves da estação de base de origem pode ser específico de múltiplas células sob controlo de múltiplas estações de base de destino. Contudo, durante a transmissão de chaves, as chaves enviadas pela estação de base de origem à estação de base de destino A só podem incluir chaves de células diferentes sob controlo da estação de base de destino A. Deste modo, a forma de realização anterior exemplar da presente invenção é igualmente aplicável ao processo de transferência do UE entre estações de base de destino diferentes.

A FIG. 3 é um fluxograma de um método para derivação de chaves de acordo com outro exemplo. Conforme ilustrado na FIG. 3, a estação de base de origem é um aparelho de rede (por exemplo, eNodeB de origem) que serve atualmente o UE, e a estação de base de destino é outro aparelho de rede (por exemplo, eNodeB de destino) selecionado pela estação de base de origem para servir o UE. O método inclui as seguintes fases:

S301. O UE envia um relatório de medição para a estação de base de origem.

S302. A estação de base de origem toma uma decisão de transferência e deriva uma chave de acordo com o ID de célula física da célula de destino obtido.

Nesta fase, é presumido que a chave derivada de acordo com o ID de célula física da célula1 de destino é KeNB*1. Vários métodos e algoritmos de derivação de chaves do estado da técnica são aplicáveis ao processo de derivação de chaves nesta fase, e não são descritos em mais pormenor.

S303. A estação de base de origem envia a KeNB*1 para a estação de base de destino.

S304. A estação de base de destino armazena a chave recebida e envia uma mensagem ACK de pedido de transferência.

S305. A estação de base de origem envia um comando de transferência para o UE.

Se o UE não puder receber o comando de transferência no caso de uma RLF, o procedimento de restabelecimento de ligação iniciado pelo UE pode incluir as seguintes fases:

S306. O UE envia um pedido de restabelecimento de ligação RRC para a estação de base de destino.

S307. Depois de a estação de base de destino receber o pedido de restabelecimento de ligação, a estação de base de

destino envia uma mensagem de restabelecimento de ligação RRC que inclui a Célula1 no pedido de transferência e deriva uma KeNB*1 utilizando a Célula1.

S308. O UE recebe a mensagem de restabelecimento de ligação RRC e deriva uma KeNB*1’ utilizando a Célula1. Deste modo, a KeNB*1’ é consistente com a KeNB*1.

Neste exemplo, a estação de base de destino pode utilizar a chave já armazenada na estação de base de destino sem voltar a derivar uma chave. O UE deriva uma chave de acordo com o ID de célula física da célula de destino fornecido pela estação de base de destino. Deste modo, as chaves utilizadas pelo UE e o aparelho de rede são as mesmas, o que garante uma comunicação normal entre o UE e o aparelho de rede, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

É compreensível para os peritos na especialidade que este exemplo seja aplicável não só ao processo de transferência do UE entre células diferentes sob controlo da mesma estação de base de destino, como também ao processo de transferência do UE entre estações de base de destino diferentes.

Além disso, é compreensível para os peritos na especialidade que o aparelho de rede e o UE neste exemplo possam chegar a um acordo antecipadamente em relação a um ou mais dos seguintes aspetos: método para derivação de chaves, método para selecionar parâmetros de derivação de chaves e método para enviar parâmetros de derivação de chaves. Neste caso, o aparelho de rede deriva uma chave de acordo com o método acordado e envia os parâmetros

necessários para o UE, enquanto o UE recebe os parâmetros necessários e deriva uma chave de acordo com o método acordado. O aparelho de rede e o UE podem determinar igualmente os métodos anteriores através de negociações. O método de negociação específico não afeta a implementação e a solução técnica e, por conseguinte, não é descrito em mais pormenor.

A FIG. 4 ilustra um aparelho para derivação de chaves de acordo com outro exemplo. O aparelho inclui:

uma unidade de receção 41 configurada para receber, pelo menos, uma chave, em que a chave é derivada de acordo com um ID de estação de base de destino e/ou um ID de célula física da célula de destino;

uma unidade de determinação 42 configurada para receber um pedido de restabelecimento RRC de um UE e selecionar uma Chave A, em que a Chave A pode ser derivada de acordo com o ID de estação de base de destino, ou de acordo com o ID de célula física da célula de destino correspondente à célula onde o UE se encontra, ou ser derivada de acordo com um ID de célula física incluído no pedido de restabelecimento RRC; e

uma unidade de envio 43 configurada para enviar o ID de estação de base de destino ou o ID de célula física da célula de destino necessário para derivar a Chave A.

A FIG. 5 ilustra um aparelho para derivação de chaves de acordo com outra forma de realização exemplar da presente invenção. O aparelho inclui:

uma unidade de acionamento 51 configurada para iniciar um procedimento de restabelecimento de ligação e acionar uma unidade de receção 52;

a unidade de receção 52 configurada para receber o ID de estação de base de destino e/ou o ID de célula física da célula de destino ao ser acionada pela unidade de acionamento 51; e

uma unidade de derivação de chaves 53 configurada para derivar uma chave de acordo com o ID de estação de base de destino ou ID de célula física da célula de destino recebido pela unidade de receção 52.

A FIG. 6 ilustra um aparelho para derivação de chaves de acordo com outra forma de realização exemplar da presente invenção. O aparelho inclui uma primeira unidade 61 e uma segunda unidade 62.

A primeira unidade 61 é configurada para receber múltiplas chaves derivadas de uma estação de base de origem, em que as múltiplas chaves correspondem a múltiplas células sob controlo de uma estação de base de destino. A segunda unidade 62 é configurada para selecionar uma chave correspondente a uma célula de destino depois de saber a célula de destino à qual o UE pede para aceder. Além disso, a chave correspondente à célula de destino selecionada pela segunda unidade 62 é derivada da estação de base de origem de acordo com o ID de célula física da célula de destino.
As chaves correspondentes às células sob controlo da estação de base de destino recebidas pela primeira unidade 61 são derivadas da estação de base de origem de acordo com os IDs de célula física da célula da estação de base de

destino. A estação de base de origem pode enviar todas as chaves derivadas de acordo com os IDs de célula física das células de destino para a estação de base de destino, de modo a que a estação de base de destino possa selecionar uma chave para ser utilizada nas comunicações com o UE de acordo com a célula à qual o UE pretende aceder. Deste modo, a taxa de sucesso de acesso do UE a novas células é de 100%. A estação de base de origem pode selecionar igualmente uma chave e enviá-la para a estação de base de destino de acordo com algumas condições; por exemplo, só pode enviar uma chave derivada de acordo com os IDs de célula física das células de destino com maior prioridade. A estação de base de origem pode derivar igualmente uma chave de acordo com algumas condições; por exemplo, só pode derivar uma chave de acordo com os IDs de célula física das células de destino com baixa prioridade e enviar as chaves para a estação de base de destino. Deste modo, a taxa de sucesso de acesso do UE aumenta e a quantidade de informações transmitidas através da estação de base de origem diminui, mas a taxa de sucesso de acesso do UE é inferior a 100%.

A primeira unidade 61 é ainda configurada para receber um pedido de restabelecimento de ligação RRC do UE.

O aparelho para derivação de chaves pode ainda incluir uma terceira unidade 63, que é configurada para enviar o ID de célula física da célula de destino ao UE.

Opcionalmente, o aparelho para derivação de chaves nesta forma de realização pode ser uma estação de base.

A FIG. 7 ilustra um sistema de comunicações de acordo com outra forma de realização exemplar da presente invenção. O sistema de comunicações inclui um aparelho 71 para derivação de chaves de acordo com a forma de realização exemplar anterior e um UE 72 que comunica com o aparelho 71.

O sistema de comunicações pode ainda incluir uma MME 73, que é configurada para: receber um ID de célula física de destino enviado pelo aparelho 71 ao UE, e encaminhar o ID de célula física de destino para o UE.

Além disso, o aparelho 71 do sistema de comunicações pode ser utilizado como a estação de base de destino do UE.

Outra forma de realização exemplar da presente invenção fornece igualmente um sistema de comunicações. O sistema de comunicações inclui um UE e um aparelho de rede.

O UE é configurado para derivar uma chave de acordo com o ID de estação de base de destino recebido ou o ID de célula física da célula de destino.

O aparelho de rede é configurado para: selecionar uma Chave A de, pelo menos, uma chave derivada de acordo com o ID de estação de base de destino e/ou o ID de célula física da célula de destino de acordo com o pedido de restabelecimento RRC recebido, e enviar o ID de estação de base de destino e o ID de célula física da célula de destino necessários para derivar uma Chave A.
O sistema de comunicações pode ainda incluir uma Entidade de Gestão de Mobilidade (MME), que é configurada para encaminhar as informações sobre a comunicação entre o

aparelho de rede e o UE. A MME encaminha o ID de estação de base de destino ou o ID de célula física da célula de destino enviado pelo aparelho de rede ao UE.

É compreensível para os peritos na especialidade que todas ou parte das fases das formas de realização anteriores possam ser implementadas através de equipamento informático que recebe instruções de um programa. O programa pode ser armazenado num meio de armazenamento legível por computador. Quando o programa é executado, são envolvidos os processos das formas de realização do método anterior. O meio de armazenamento anterior pode ser um disco magnético, um disco compacto (CD), uma memória só de leitura (ROM) ou uma memória de acesso aleatório (RAM).

Nas formas de realização da presente invenção, o aparelho de derivação de chaves e o sistema de comunicações podem assegurar que o UE e o aparelho de rede utilizam a mesma chave, o que garante uma comunicação normal entre o UE e o aparelho de rede, reduz a taxa de queda de chamadas e origina uma melhor experiência de utilizador.

Embora a invenção tenha sido descrita através de diversas formas de realização exemplares, a invenção não se limita a estas formas de realização.

Lisboa, 22 de Maio de 2012

REIVINDICAÇÕES

1. Um método para derivação de chaves, caracterizado por:
receber (S203), através de uma estação de base de destino, múltiplas chaves derivadas de uma estação de base de origem, em que as múltiplas chaves correspondem a múltiplas células sob controlo da estação de base de destino;
receber (S206), através da estação de base de destino, um pedido de restabelecimento de ligação de controlo de recurso de rádio (RRC) de um Equipamento de Utilizador (UE); e
selecionar, através de uma estação de base de destino, uma chave das múltiplas chaves recebidas pela estação de base de destino para ser utilizada na comunicação com o UE, sendo que a chave selecionada corresponde a um célula de destino à qual o UE pede para aceder durante o procedimento de restabelecimento de ligação RRC.

2. O método de acordo com a reivindicação 1, caracterizado por as múltiplas chaves serem derivadas de acordo com identificadores (IDs) de célula física das células sob controlo da estação de base de destino.

3. O método de acordo com a reivindicação 1 ou 2, caracterizado por:
as múltiplas chaves serem todas, ou parte delas, derivadas da estação de base de origem de acordo com os IDs de célula física de todas as células sob controlo da estação de base de destino, sendo que parte das chaves é selecionada e enviada para a estação de base de destino pela estação de base de origem de acordo com uma condição predefinida; ou
as múltiplas chaves serem derivadas da estação de base de origem de acordo com os IDs de célula física das células com maiores prioridades da estação de base de destino.

4. O método de acordo com a reivindicação 1, caracterizado por a receção (S203), através da estação de base de destino, das múltiplas chaves enviadas pela estação de base de origem compreender:
a receção, através da estação de base de destino, de uma mensagem de nível de acesso compreendendo as múltiplas chaves enviadas pela estação de base de origem; ou
a receção, através da estação de base de destino, de uma mensagem de uma interface S1, a mensagem compreendendo as múltiplas chaves enviadas por uma Entidade de Gestão de Mobilidade (MME), em que as múltiplas chaves são fornecidas à MME pela estação de base de origem.

5. O método de acordo com a reivindicação 1, caracterizado por compreender ainda:
o envio, através da estação de base de destino, de um ID de célula física da célula de destino ao UE.

6. O método de acordo com a reivindicação 5, caracterizado por o envio, através da estação de base de destino, do ID de célula física da célula de destino ao UE compreender:
o envio, através da estação de base de destino, da difusão do sistema compreendendo o ID de célula física da célula de destino ao UE; ou
o envio, através da estação de base de destino, de uma mensagem de restabelecimento de ligação RRC compreendendo o ID de célula física da célula de destino ao UE.

7. Um aparelho numa estação de base que funciona como uma estação de base de destino para um Equipamento de Utilizador (UE), caracterizado por:
uma primeira unidade (61) configurada para receber múltiplas chaves derivadas de uma estação de base de

origem, sendo que as múltiplas chaves correspondem a múltiplas células sob controlo de uma estação de base de destino, em que a primeira unidade (61) é ainda configurada para receber uma mensagem de pedido de restabelecimento de ligação de Controlo de Recurso de Rádio (RRC) de um UE; e uma segunda unidade (62) configurada para selecionar uma chave a partir das múltiplas chaves recebidas pela estação de base de destino para ser utilizada na comunicação com o UE, sendo que a chave selecionada corresponde a uma célula de destino à qual o UE pede para aceder durante o procedimento de restabelecimento de ligação RRC.

8. O aparelho de acordo com a reivindicação 7, caracterizado por as múltiplas chaves serem derivadas de acordo com identificadores (IDs) de célula física das células sob controlo da estação de base de destino.

9. O aparelho de acordo com a reivindicação 7 ou 8, caracterizado por:
as múltiplas chaves serem todas, ou parte delas, derivadas da estação de base de origem de acordo com os IDs de célula física de todas as células sob controlo da estação de base de destino; em que parte das chaves é selecionada e enviada para a estação de base de destino pela estação de base de origem de acordo com uma condição predefinida; ou
as múltiplas chaves serem derivadas da estação de base de origem de acordo com os IDs de célula física das células com uma prioridade da estação de base de destino.

10. O aparelho de acordo com a reivindicação 7, caracterizado por a chave correspondente à célula de destino ser derivada da estação de base de origem de acordo com um ID de célula física da célula de destino.

11. O aparelho de acordo com a reivindicação 7, caracterizado por compreender ainda:
uma terceira unidade (63) configurada para enviar um ID de célula física da célula de destino ao UE.

12. Um aparelho numa estação de base que funciona como uma estação de base de origem para um Equipamento de Utilizador (UE), caracterizado por:
meios para derivar múltiplas chaves correspondentes a múltiplas células sob controlo de uma estação de base de destino; e
meios para enviar as múltiplas chaves para a estação de base de destino.

13. O aparelho de acordo com a reivindicação 12, caracterizado por as múltiplas chaves serem derivadas de acordo com os IDs de célula física das células sob controlo da estação de base de destino.

14. O aparelho de acordo com a reivindicação 12, caracterizado por o transmissor ser configurado para enviar as múltiplas chaves num pedido de transferência através de uma interface X2.

15. Um sistema de comunicações caracterizado por compreender o aparelho de acordo com qualquer uma das reivindicações 7 a 11, e um Equipamento de Utilizador em comunicação com o aparelho.

Lisboa, 22 de Maio de 2012

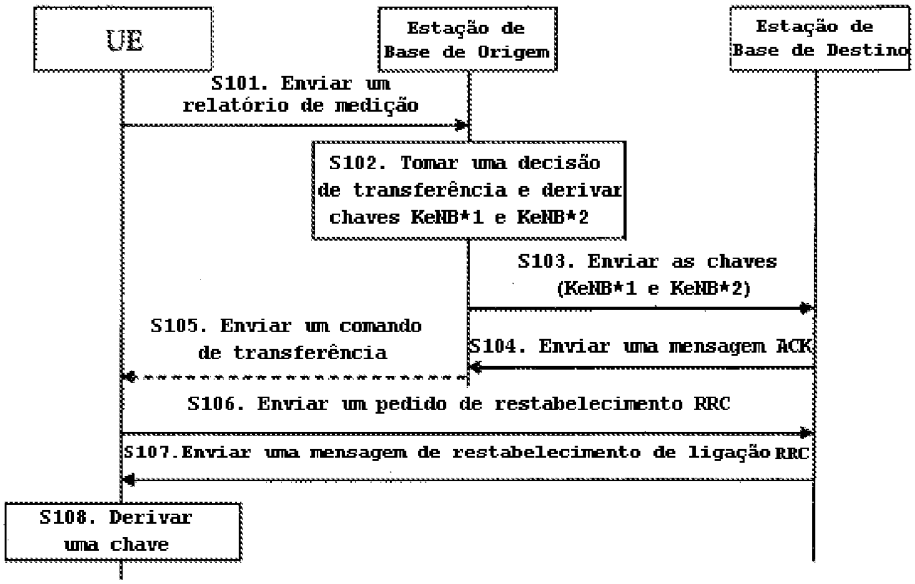
UE
Estação de Base de Origem
Estação de Base de Destino
S101. Enviar um relatório de medição
S102. Tomar uma decisão de transferência e derivar chaves KeNB*1 e KeNB*2
S103. Enviar as chaves (KeNB*1 e KeNB*2)
S105. Enviar um comando de transferência
S104. Enviar uma mensagem ACK
S106. Enviar um pedido de restabelecimento RRC
S107.Enviar uma mensagem de restabelecimento de ligação RRC
S108. Derivar uma chave

FIG. 1

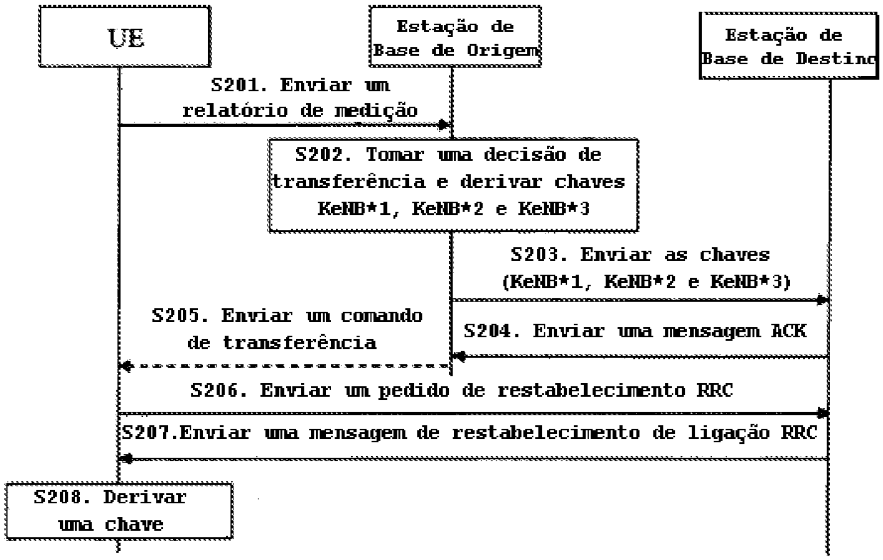
UE
Estação de Base de Origem
Estação de Base de Destino
S201. Enviar um relatório de medição
S202. Tomar uma decisão de transferência e derivar chaves KeNB*1, KeNB*2 e KeNB*3
S203. Enviar as chaves (KeNB*1, KeNB*2 e KeNB*3)
S205. Enviar um comando de transferência
S204. Enviar uma mensagem ACK
S206. Enviar um pedido de restabelecimento RRC
S207.Enviar uma mensagem de restabelecimento de ligação RRC
S208. Derivar uma chave

FIG. 2

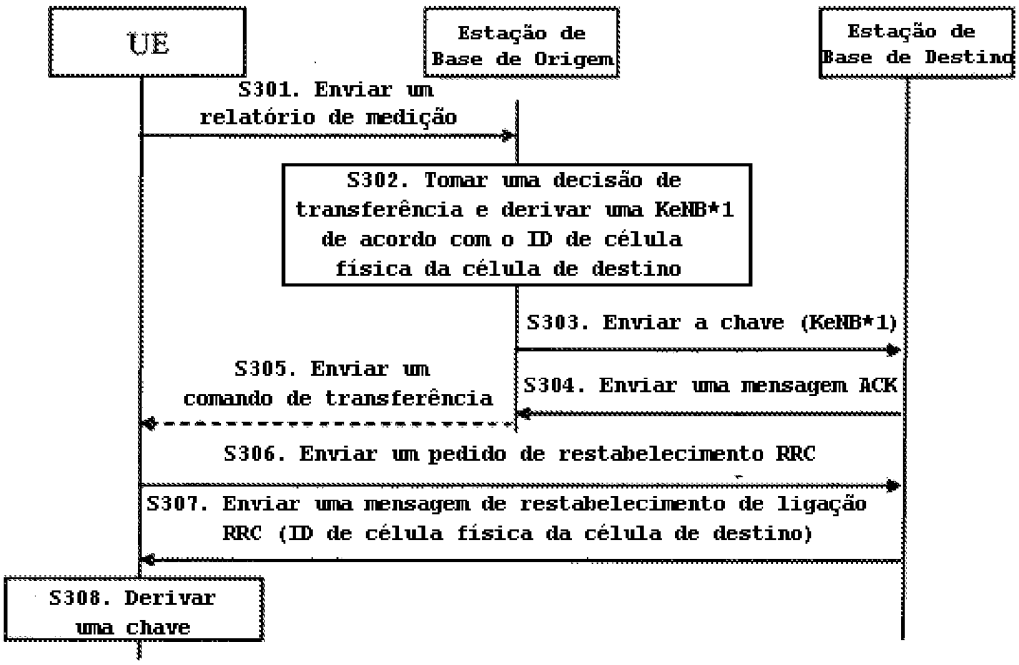
UE
Estação de Base de Origem
Estação de Base de Destino
S301. Enviar um relatório de medição
S302. Tomar uma decisão de transferência e derivar uma KeNB*1 de acordo com o ID de célula física da célula de destino
S303. Enviar a chave (KeNB*1)
S304. Enviar uma mensagem ACK
S305. Enviar um comando de transferência
S306. Enviar um pedido de restabelecimento RRC
S307. Enviar uma mensagem de restabelecimento de ligação RRC (ID de célula física da célula de destino)
S308. Derivar uma chave

FIG. 3

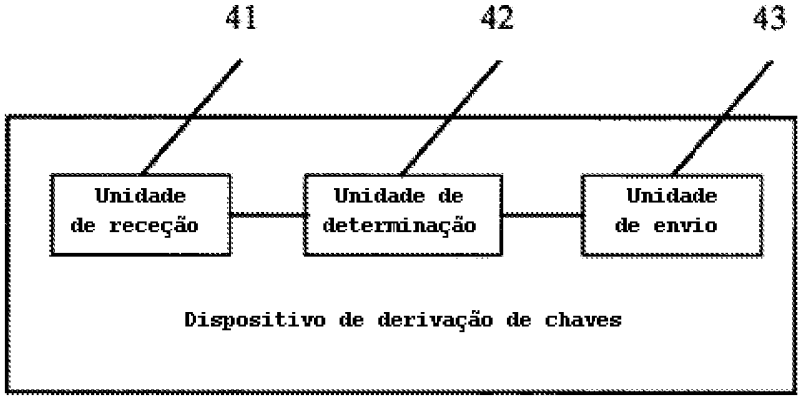
41
42
43
Unidade de receção
Unidade de determinação
Unidade de envio
Dispositivo de derivação de chaves

FIG. 4

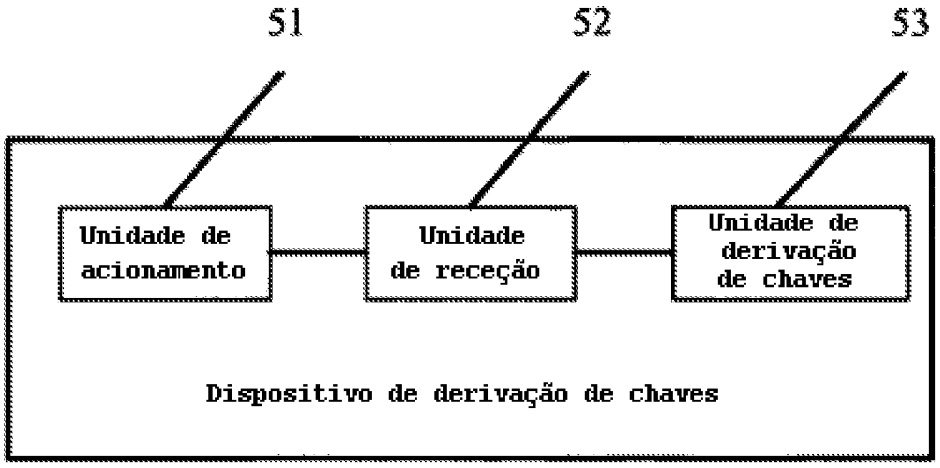
51
52
53
Unidade de acionamento
Unidade de receção
Unidade de derivação de chaves
Dispositivo de derivação de chaves

FIG. 5

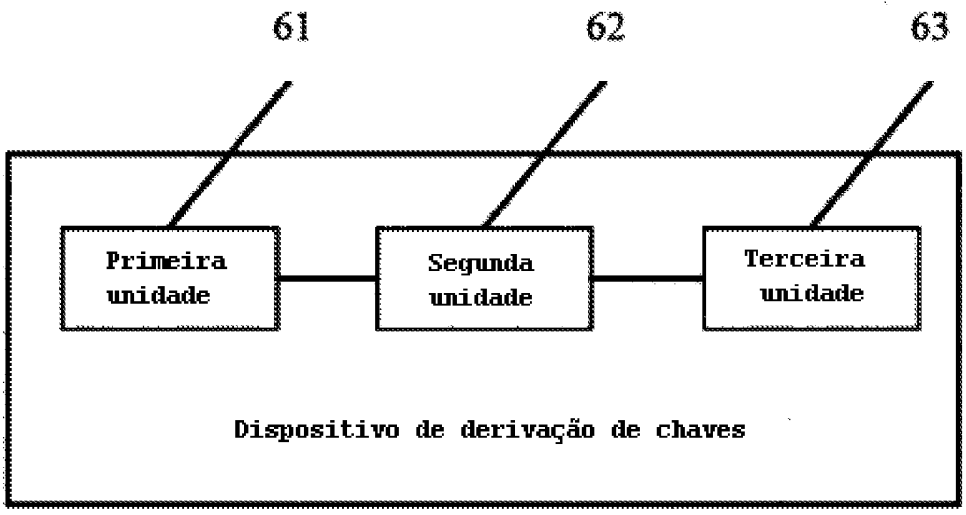
61
62
63
Primeira unidade
Segunda unidade
Terceira unidade
Dispositivo de derivação de chaves

FIG. 6

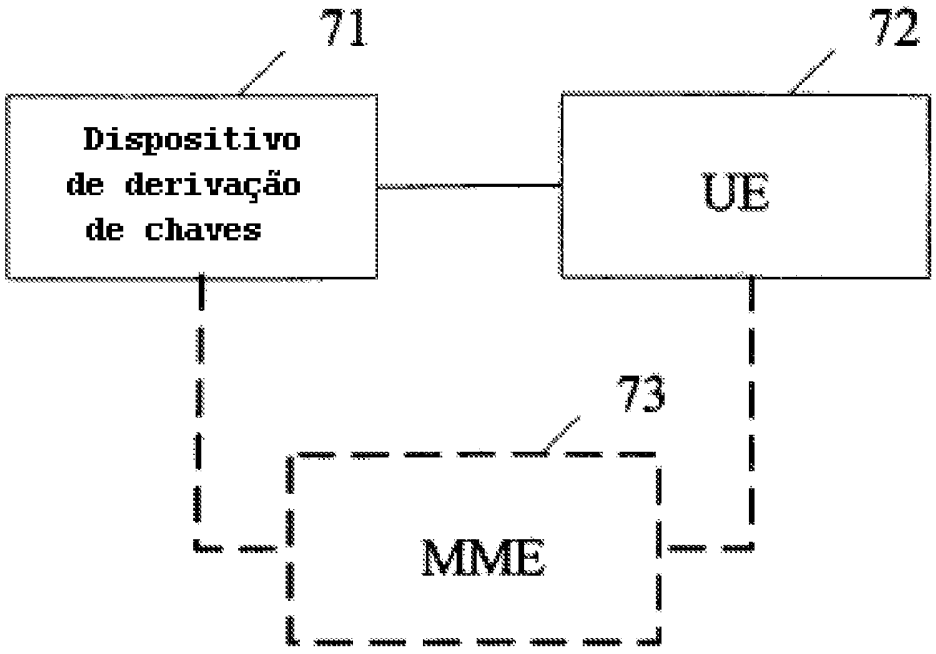

FIG. 7