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

**(11) PI 0822761-6 B1**

**(22) Data do Depósito:** 21/07/2008

**(45) Data de Concessão:** 29/09/2020

**(54) Título:** MÉTODO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA PROTEGER COMUNICAÇÃO ENTRE DUAS ENTIDADES, MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR, DISPOSITIVO ADAPTADO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA UMA ENTIDADE DE COMUNICAÇÕES, EQUIPAMENTO DE USUÁRIO, E, SISTEMA

**(51) Int.Cl.:** H04L 9/08; H04L 9/32; H04W 12/04; H04W 12/06.

**(52) CPC:** H04L 9/0866; H04L 9/0869; H04L 9/0891; H04L 9/3271; H04W 12/04; (...).

**(30) Prioridade Unionista:** 06/06/2008 US 61/059386.

**(73) Titular(es):** TELEFONAKTIEBOLAGET LM ERICSSON (PUBL).

**(72) Inventor(es):** KARL NORRMAN; MATS NÄSLUND.

**(86) Pedido PCT:** PCT EP2008005960 de 21/07/2008

**(87) Publicação PCT:** WO 2009/146729 de 10/12/2009

**(85) Data do Início da Fase Nacional:** 03/12/2010

**(57) Resumo:** MÉTODO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA PROTEGER COMUNICAÇÃO ENTRE DUAS ENTIDADES, PRODUTO DE PROGRAMA DE COMPUTADOR, DISPOSITIVO ADAPTADO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA UMA ENTIDADE DE COMUNICAÇÕES, EQUIPAMENTO DE USUÁRIO,E, SISTEMA. Uma técnica para gerar uma chave criptográfica (120) é provida. A técnica é particularmente útil para proteger a comunicação entre duas entidade (202,302,204,304) correndo cooperativamente uma operação de segurança distribuída. A técnica inclui prover pelo menos dois parâmetros (106, 108), o primeiro parâmetro (106) incluindo ou derivando de algumas chaves criptográficas (110,112) que foram computadas pela primeira entidade (202,302) correndo a operação de segurança e o segundo parâmetro (108) incluindo ou derivando de um passe(116) tendo um valor diferente cada vez que a operação de segurança (114) é iniciada pela segunda entidade(204,304) para a primeira entidade (202,302). Uma função de derivação chave é aplicada aos parâmetros providos (106,108) para gerar a chave criptográfica desejada (120).

# MÉTODO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA PROTEGER COMUNICAÇÃO ENTRE DUAS ENTIDADES, MEIO DE ARMAZENAMENTO LEGÍVEL POR COMPUTADOR, DISPOSITIVO ADAPTADO PARA GERAR UMA CHAVE CRIPTOGRÁFICA PARA UMA ENTIDADE DE COMUNICAÇÕES, EQUIPAMENTO DE USUÁRIO, E, SISTEMA

## Campo Técnico

[001] A presente invenção relaciona-se geralmente a uma técnica para gerar chaves criptográficas. Particularmente, a invenção relaciona-se a uma técnica de geração de chave criptográfica que provê um alto nível de segurança.

## Fundamento

[002] O protocolo de Autenticação e Acordo de Chave (AKA) é um protocolo baseado em intimação-resposta que usa criptografia simétrica. As metas principais de AKA incluem autenticação mútua por duas entidades se comunicando entre si e estabelecimento de chaves criptográficas para proteger a comunicação trocada entre elas. Uma variante de AKA é o UMTS (do inglês, *Universal Mobile Telecommunication System*) AKA, incluído na arquitetura de segurança padronizada por 3GPP para redes de comunicação móveis 3G na Especificação Técnica 3G TS 33.102.

[003] O conceito básico de UMTS AKA é mostrado na Figura 1. Se referindo a esta figura, o protocolo de UMTS AKA é corrido entre um equipamento de usuário (UE) e uma entidade de rede (NE). A entidade de rede inicia o AKA enviando um pedido de autenticação de usuário ao UE. Junto com o pedido, uma intimação aleatória, ou código aleatório (RAND), e um Passe de Autenticação (AUTN) são enviados ao UE. Na recepção do RAND e do AUTN, o UE, entre outras coisas, computa uma Chave de Cifra (CK) e uma Chave de Integridade (IK) e então as usa para funções de cálculo e integridade.

[004] O 3GPP também está empreendendo a padronização de denominadas redes de comunicação "além de 3G". Evolução de Arquitetura de Sistema (SAE) e Avaliação de Longo Prazo (LTE) são dois aspectos relacionados proximamente da rede além de 3G. Comparada com redes 3G convencionais, uma rede baseada em SAE/LTE pode impor exigências de segurança mais altas e/ou mais. Por exemplo, mais chaves criptográficas para assegurar a comunicação a níveis diferentes podem ser precisadas. O 3GPP, em outro documento relacionado a padrão, 3GPP TR 33.821, recomendou uma hierarquia de chave para derivar mais chaves criptográficas para uso em SAE/LTE.

[005] Figura 2 mostra esta hierarquia de chave. Ao mesmo topo da hierarquia está uma chave K, uma chave criptográfica de longo prazo compartilhada entre o Módulo de Identidade de Assinante Universal (USIM) do UE e o Centro de Autenticação (AuC) residindo na rede. Um nível abaixo é um par de chaves criptográficas CK e IK que são derivadas pelo UE, particularmente pelo USIM disso, de uma mesma maneira ou semelhante como a operação de UMTS AKA mencionada acima. Adicionalmente abaixo na hierarquia está uma chave $K_{ASME}$ que é derivada pelo UE de CK, IK, e, se necessário, alguns outros parâmetros. Uma vez derivada, $K_{ASME}$ é transferida de AuC à rede de acesso, particularmente para a Entidade de Administração de Segurança de Acesso (ASME) da rede de SAE/LTE, e então compartilhada entre o UE e a rede. Quando a rede de acesso está baseada em tecnologia de LTE, as funcionalidades do ASME são operadas por uma Entidade de Administração de Mobilidade (MME).

[006] A chave $K_{ASME}$, e as chaves "abaixo" dela na hierarquia, podem ser derivadas aplicando uma certa função criptográfica. Por exemplo,

$K_{ASME}$ = KDF(CK || IK, 0x02 || PLMN_ID || <other_parameter>)

onde KDF está baseada em uma função de derivação de chave

(KDF) de Arquitetura de 'Bootstrapping' Genérica (GBA). Uma GBA KDF está especificada em 3G TS 33.220.

[007] A GBA KDF pode fazer uso de funções de reedição criptográficas tais como as funções de reedição de Algoritmo de Reedição Segura (SHA). Entre muitas funções de reedição de SHA, SHA-256 é uma variante altamente segura desde que é considerada resistente à colisão e atua como uma função pseudo-aleatória. Como seu nome sugere, SHA-256 é uma função de reedição de Algoritmo de Reedição Segura com um comprimento sumário (saída) de 256 bits. O PLMN_ID é um identificador da rede servindo o UE.

[008] Foi percebido que, a fim de alcançar um alto nível de segurança, não é suficiente basear a função de GBA KDF principalmente em CK e IK somente. A razão para isto é o risco que um dado UE poderia obter a mesma CK duas vezes, ou dois UEs diferentes podem obter a mesma CK. Em tais casos, a "singularidade" das entradas para a KDF é indeterminada, e uma colisão entre UEs diferentes (usando a mesma $K_{ASME}$) pode ocorrer.

[009] Como uma observação geral, enquanto é certo que KDF(x) produz a mesma chave como KDF(y) se x = y, a conversação não pode sempre se manter. Quer dizer, até mesmo se $x \neq y$, ainda pode acontecer que KDF(x) = KDF(y). Porém, este é um evento improvável desde que a KDF é recomendada ser baseada em SHA-256 que, como mencionado, foi projetado para ser resistente à colisão. Assim, para a técnica descrita aqui, pode ser assumido seguramente que KDF(x) = KDF(y) se e somente se x = y. Esta suposição permite a técnica descrita aqui ser focalizada em assegurar "singularidade" das entradas à KDF.

[0010] O corpo de padronização da especificação de GBA KDF (ETSI/SAGE, o Grupo de Peritos de Algoritmo Especial) notou o problema anterior e recomendou incluir a Identidade de Usuário Privado (IMPI) do UE em <other_parameter> para evitar colisões entre UEs diferentes. Como uma

recomendação adicional, um código aleatório tal como o RAND também pode ser incluído em <other_ parameter>. Isto é descrito em uma declaração de ligação de ETSI/SAGE para 3GPP SA3 (em número de documento 3GPP S3 - 030219).

[0011] Porém, foi achado que as recomendações anteriores ainda não podem garantir a "singularidade" das entradas à KDF. Isto pode ser visto da análise abaixo da propriedade de segurança da função GBA KDF e seu uso em SAE/LTE para um e o mesmo UE (por exemplo um e o mesmo IMPI).

[0012] Primeiramente, a construção básica seguinte é considerada:

KDF(CK, IMPI).

[0013] Desde que foi assumido que IMPI = IMPI' (quando o UE é fixo), esta construção básica conduzirá à colisão para duas entradas (CK, IMPI), (CK, IMPI') se e somente se CK = CK'.

[0014] Secundariamente, outra construção é considerada, que está mais perto de GBA KDF atual:

KDF(CK || IK, IMPI).

[0015] Porém, incluir IK nas entradas não muda a propriedade de colisão anterior como alguém poderia acreditar em princípio. Quer dizer, KDF(CK || IK, IMPI) será igual para KDF(CK' || IK', IMPI) se e somente se CK = CK'. Para entender por que incluir IK não ajudaria, é necessário considerar como CK e IK são produzidas pelo algoritmo criptográfico executado no UE.

[0016] Um algoritmo criptográfico de lado de UE típico é o algoritmo de Milenage, que é mostrado na Figura 9. Na Figura 9, Ek denota o algoritmo de Padrão de Criptografia Avançada (AES), também conhecido como o algoritmo de Rijndael, usando a chave K (armazenada no AuC e USIM de UE). Considere agora o que acontece se CK = CK'. Desde que AES é uma permutação (um mapeamento de um para um), isto implica que o valor intermediário (ocorrendo na seta grossa) é determinado exclusivamente pelo

resultado de f3 que acontece ser CK. Mas isto implica que o valor na seta grossa ao produzir CK deve ser igual ao valor ocorrendo no mesmo lugar quando CK' era produzida. Isto por sua vez significa que os valores ocorrendo como entrada a f4 devem ser os mesmos e conseqüentemente, os mesmos valores de f4 devem ocorrer. Como acontece, f4 é IK. Assim, foi mostrado que CK = CK' se e somente se IK = IK'.

[0017] A seguir, uma construção "melhorada" de acordo com a recomendação do corpo de padronização (SAGE), isto é, incluindo RAND nas entradas, é considerado:

$$KDF(CK || IK, RAND || IMPI).$$

[0018] Assuma que CK = CK' (e assim IK = IK'). É esperado que o uso de RAND garantirá singularidade. Porém, isto não é verdade. Considere novamente a parte "pertinente" do algoritmo de Milenage que produzia CK e IK de RAND: Como mostrado na Figura 9, há uma situação na qual o valor na seta grossa correspondendo a RAND é igual àquele correspondendo a RAND. Mas novamente, AES (Ek) é uma permutação de forma que as entradas também devem ser iguais, isto é, RAND = RAND'. (O fato que AES é dependente de K não ajuda desde que um UE fixo é assumido e assim a mesma K ocorrerá em ambos os casos.)

[0019] Em outras palavras, foi mostrado que (CK || IK, RAND || IMPI) = (CK' || IK', RAND' || IMPI) se e somente se RAND = RAND'. No caso de SAE/LTE, o PLMN_ID também pode ser incluído nas entradas, mas desde que é altamente provável que o UE fica na mesma rede várias vezes, este parâmetro PLMN_ID não pode ser confiado para o propósito de garantir singularidade.

[0020] Uma abordagem alternativa para tentar evitar colisão poderia ser usar outro algoritmo que não AES para o processamento criptográfico dos algoritmos de f3 e f4. Especificamente, a análise acima era baseada no fato que AES é uma permutação. Seria portanto possível usar uma não permutação

(mapeamento de muitos para um) em vez de AES. Isto é problemático por duas razões. Em primeiro lugar, USIMs existentes devem ser adaptados para serem adequados para a arquitetura de 3GPP SAE. Secundariamente, escolhendo uma função de não permutação, alguém na verdade aumenta a probabilidade que duas saídas de por exemplo f3 colidirão.

[0021] A falta de singularidade das entradas pode ser um assunto de segurança sério. Desde que colisão ocorrerá se e somente se RAND = RAND', e desde que RAND é 128 bits, a colisão é esperada ocorrer depois de cerca de $2^{(128/2)} = 2^{64}$ autenticações (isto é o denominado "paradoxo de aniversário"). Claramente, isto é mais baixo que o nível de segurança visado de GBA (que é 128 bits). Para LTE o caso é até pior, desde que LTE é exigido prover um nível de segurança de 256 bits. Assim, a alta probabilidade de colisão é um obstáculo significante para prover o nível de segurança exigido em SAE/LTE.

Sumário

[0022] Por conseguinte, há uma necessidade por uma solução que evite as colisões mencionadas acima. A solução também deveria trabalhar idealmente com USIMs já desdobrados e não requerer substituir todos os USIMs.

[0023] De acordo com um primeiro aspecto, é provido um método para gerar uma chave criptográfica. A chave criptográfica é usada para, entre outros, proteger a comunicação entre duas entidades. O método é executado pela primeira entidade. O método faz parte de uma operação de segurança distribuída que é iniciada pela segunda entidade. O método inclui prover pelo menos dois parâmetros, em que o primeiro parâmetro tanto inclui ou é derivado de um conjunto de chaves criptográficas que foram computadas pela primeira entidade correndo a operação de segurança; e o segundo parâmetro tanto inclui ou é derivado de um passe tendo um valor diferente cada vez que a operação de segurança é iniciada pela segunda entidade para a primeira

entidade (em outras palavras, o valor do passe nunca é o mesmo para qualquer duas operações de segurança); e aplicar uma função de derivação de chave para gerar uma chave criptográfica baseada nos parâmetros providos.

[0024] A expressão "um parâmetro inclui X" pode significar que a variável X, em seu formato de sequência, forma o parâmetro ou uma parte disso. A expressão "um parâmetro é derivado de X" pode significar que o parâmetro é o resultado de aplicar certas funções, tais como funções matemáticas, pelo menos à variável X. Exemplos das funções incluem, mas não estão limitados a, operações aritméticas, operações lógicas, operações de sequência, e qualquer combinação disso. A operação aritmética pode ser adição, subtração, multiplicação, etc., e qualquer combinação significante disso. A operação lógica pode ser E, OU, OU Exclusivo (xOR), NÃO, etc., e qualquer combinação significante disso. A operação de sequência pode ser Concatenação, Inversão, Substituição, etc., e qualquer combinação significante disso. Adicionalmente, a operação aritmética, a operação lógica e a operação de sequência podem ser combinadas.

[0025] Particularmente, o passe mencionado acima pode incluir ou ser derivado de um número de seqüência (SQN) indicando o número de vezes que a operação de segurança foi iniciada pela segunda entidade para a primeira entidade. Com cada iniciação, o SQN pode ser incrementado pela segunda entidade. Este mecanismo assegura que o passe tenha um valor diferente por cada operação de segurança iniciada.

[0026] O passe pode levar muitas formas. Em um caso, o próprio SQN pode ser o passe. Alternativamente, o passe pode ser derivado do SQN usando um algoritmo envolvendo certas operações matemáticas, tal como pelo menos uma de uma operação aritmética, uma operação lógica e uma operação de sequência. Por exemplo, o passe pode incluir ou ser derivado de um Passe de Autenticação (AUTN) construído pela segunda entidade baseado no SQN e entregue à primeira entidade. Esta construção e entrega podem fazer parte da

operação de segurança.

[0027] Especificamente, o passe pode incluir um OU exclusivo do SQN e uma Chave de Anonimato (AK). Mais especificamente, o passe pode ser uma concatenação do OU exclusivo do SQN e a Chave de Anonimato (AK), um Campo de Autenticação e Administração de Chave (AMF), e um Código de Autenticação de Mensagem (MAC). Esta concatenação pode ser expressa como:

$$\text{passe} = \text{AUTN} = (\text{SQN xOR AK}) \,||\, \text{AMF} \,||\, \text{MAC}$$

ou

$$\text{passe} = \text{função (AUTN)} = \text{função ((SQN xOR AK)} \,||\, \text{AMF} \,||\, \text{MAC)}$$

[0028] O segundo parâmetro pode adicionalmente incluir ou ser derivado de uma intimação aleatória, ou código aleatório (RAND). O RAND pode ser gerado pela segunda entidade e entregue à primeira entidade como parte da operação de segurança. O segundo parâmetro ainda pode incluir adicionalmente ou ser derivado de um identificador da primeira entidade. Este identificador pode ser uma Identidade de Usuário Privada (IMPI) ou uma Identidade de Assinante Móvel Internacional (IMSI). Até mesmo adicionalmente, o segundo parâmetro pode incluir ou ser derivado de um identificador de uma rede de comunicação e particularmente a rede de serviço da primeira entidade. Por exemplo, este identificador poderia ser um Identificador de Rede Móvel Terrestre Pública (PLMN_ID).

[0029] Especificamente, o segundo parâmetro pode incluir ou ser derivado de uma concatenação de 0x02, um PLMN_ID, um RAND, um IMPI ou IMSI, e o passe. Isto poderia ser expresso como:

$$0x02 \,||\, \text{PLMN\_ID} \,||\, \text{RAND} \,||\, \text{IMPI} \,||\, \text{passe.}$$

Quando o passe é o próprio SQN, o anterior se torna:

$$0x02 \,||\, \text{PLMNJD} \,||\, \text{RAND} \,||\, \text{IMPI} \,||\, \text{SQN;}$$

e quando o passe é o AUTN, o anterior se torna:

$$0x02 \,||\, \text{PLMN\_ID} \,||\, \text{RAND} \,||\, \text{IMPI} \,||\, \text{AUTN.}$$

[0030] Com respeito ao primeiro parâmetro usado no método, este parâmetro inclui ou é derivado de um conjunto de chaves criptográficas que foram obtidas pela primeira entidade correndo a operação de segurança. O conjunto de chaves criptográficas pode incluir ou ser derivado de uma Chave de Cifra (CK) e uma Chave de Integridade (IK).

[0031] A CK e IK podem ser a chave de cifra e chave de integridade computadas pela primeira entidade baseado em um AUTN e um RAND. AUTN e o RAND podem ser entregues da segunda entidade. Esta computação como também a entrega do AUTN e do RAND podem fazer parte da operação de segurança.

[0032] Em uma implementação, o primeiro parâmetro pode incluir ou ser derivado de uma concatenação de CK e IK. Isto pode ser expresso matematicamente como:

$$CK \,||\, IK.$$

[0033] O método descrito aqui gera uma chave criptográfica. Esta chave pode ser compartilhada pelo menos pela primeira entidade e pela segunda entidade, em qualquer comunicação subseqüente entre elas. Em certas implementações, esta chave pode ser a $K_{ASME}$ referida na "hierarquia de chave" da Figura 2, que pode ser compartilhada pela primeira entidade e uma Entidade de Administração de Acesso de Segurança (ASME) da segunda entidade.

[0034] O método pode ser estendido para incluir aplicar um ou mais funções de derivação de chave adicionais para gerar mais chaves criptográficas. Tal geração é baseada em, ou faz uso da chave criptográfica gerada no método não estendido básico descrito acima, por exemplo $K_{ASME}$.

[0035] As chaves criptográficas geradas pelo método estendido podem incluir pelo menos um de um conjunto de chaves criptográficas para proteger o tráfego de Camada Sem Acesso (NAS); um conjunto de chaves criptográficas para a proteção de tráfego de Controle de Recurso de Rádio

(RRC); um conjunto de chaves criptográficas para a proteção de tráfico de Plano de Usuário (UP); e uma chave criptográfica intermediária, tal como $K_{eNB}$, para derivar as chaves criptográficas para proteger o tráfego de RRC e/ou as chaves criptográficas para proteger o tráfego de UP. Para uma compreensão mais fácil destas chaves, referência é feita à Figura 2 que ilustra a hierarquia chave usada em SAE/LTE.

[0036] Especificamente, o conjunto de chaves criptográficas para proteger o tráfego de NAS pode incluir uma chave para proteger o tráfego de NAS com um algoritmo de criptografia ($K_{NASenc}$) e/ou outra chave para proteger o tráfego de NAS com um algoritmo de integridade ($K_{NASint}$). Semelhantemente, o conjunto de chaves criptográficas para a proteção de tráfego de RRC pode incluir uma chave para proteger o tráfego de RRC com um algoritmo de criptografia ($K_{RRCenc}$) e/ou outra chave para proteger o tráfego de RRC com um algoritmo de integridade ($K_{RRCint}$). Adicionalmente, o conjunto de chaves criptográficas para a proteção de tráfego de UP pode incluir uma chave para proteger o tráfego de UP com um algoritmo de criptografia ($K_{UPenc}$).

[0037] Para a técnica descrita aqui, a "primeira entidade" pode ser um equipamento de usuário, tal como uma estação móvel. A "segunda entidade" pode ser uma entidade localizada dentro de uma rede de comunicação, conseqüentemente uma "entidade de rede". Particularmente, a segunda entidade pode estar localizada em uma rede de SAE/LTE.

[0038] A segunda entidade pode incluir um Centro de Autenticação (AuC)/Servidor de Assinante Doméstico (HSS) e uma Entidade de Administração de Mobilidade (MME). A MME pode ser responsável pela iniciação da operação de segurança para a primeira entidade. As chaves criptográficas geradas podem ser geradas pelo AuC/HSS e serem compartilhadas pela primeira entidade e a MME. O AuC/HSS pode incrementar o SQN, particularmente cada vez que a operação de segurança é

iniciada para a primeira entidade. Adicionalmente, o AuC/HSS também pode construir o AUTN baseado no SQN.

[0039] A operação de segurança referida aqui pode ser executada pela primeira e segundas entidades de uma maneira cooperativa. Por exemplo, a operação de segurança pode estar baseada em um procedimento de AKA, tal como o protocolo de UMTS AKA.

[0040] A função de derivação de chave referida pelo método pode ser uma função de derivação chave de Arquitetura de 'Bootstrapping' Genérica (GBA). Uma função de derivação chave de Arquitetura de 'Bootstrapping' Genérica pode empregar um função de reedição de Algoritmo de Reedição Segura (SHA). Em particular, uma função de reedição de Algoritmo de Reedição Segura com um sumário de um comprimento de 256 bits (SHA-256) pode ser empregada.

[0041] De acordo com outro aspecto, um produto de programa de computador é provido. O produto de programa de computador inclui porções de código de programa para executar as etapas do método descrito aqui quando o produto de programa de computador é executado em um sistema de computador para um dispositivo de computação. O produto de programa de computador pode ser armazenado em um meio de informação legível por computador.

[0042] Em geral, a solução pode ser praticada por meio de hardware, software, ou uma abordagem de hardware/software combinada.

[0043] Como para uma realização de hardware, um dispositivo adaptado para gerar uma chave criptográfica para uma entidade de comunicações é provido. O dispositivo pode executar uma operação de segurança, da qual a geração da chave criptográfica pode fazer parte disso. O dispositivo inclui um primeiro componente adaptado para prover pelo menos dois parâmetros, em que o primeiro parâmetro pode incluir ou ser derivado de um conjunto de chaves criptográficas tendo sido computadas pela entidade de

comunicações correndo a operação de segurança, e o segundo parâmetro pode incluir ou ser derivado de um passe tendo um valor diferente cada vez que a operação de segurança é iniciada para a entidade de comunicações. O dispositivo adicionalmente inclui um segundo componente adaptado para executar uma função de derivação de chave para gerar uma chave criptográfica baseada nos parâmetros providos. Como dito acima, o passe pode levar muitas formas possíveis.

[0044] O passe pode incluir ou ser derivado de um SQN indicando o número de vezes que a operação de segurança foi iniciada para a entidade de comunicações. Em uma implementação, o próprio SQN é o passe. Alternativamente, o passe pode ser derivado do SQN usando um algoritmo envolvendo pelo menos uma de operação aritmética, operação lógica e operação de sequência. Por exemplo, o passe pode incluir ou ser derivado de um AUTN que é construído baseado no SQN e entregue à entidade de comunicações, em que esta construção e entrega fazem parte da operação de segurança. Por exemplo, o passe pode ser uma concatenação do OU Exclusivo do SQN e uma Chave de Anonimato (AK), um Campo de Autenticação e Administração de Chave (AMF), e um Código de Autenticação de Mensagem (MAC). Especificamente, isto pode ser expresso como:

$$\text{passe} = \text{AUTN} = (\text{SQN xOR AK}) \,||\, \text{AMF} \,||\, \text{MAC}.$$

[0045] Além do passe, o segundo parâmetro também pode incluir ou ser derivado de um RAND. O RAND pode ser entregue à entidade de comunicações como parte da operação de segurança. Adicionalmente, o segundo parâmetro pode incluir ou ser derivado de um identificador da entidade de comunicações. Um exemplo do identificador é uma Identidade de Usuário Privada (IMPI) da entidade de comunicações. Até mesmo adicionalmente, o segundo parâmetro pode incluir ou ser derivado de um identificador da rede de serviço da entidade de comunicações. Este

identificador poderia ser uma Identificador de Rede Móvel Terrestre Pública (PLMN_ID).

[0046] Um exemplo particular do segundo parâmetro pode incluir ou ser derivado de uma concatenação de 0x02, um PLMN_ID, um RAND, uma IMPI ou uma IMSI, e o passe. Por exemplo, o segundo parâmetro pode ser expresso como:

0x02 ||PLMN_ID || RAND || IMPI || passe.

Quando passe é o SQN, o anterior se torna:

0x02 || PLMN_ID || RAND || IMPI || SQN;

e quando o passe é AUTN, o anterior se torna:

0x02 || PLMNJD ||RAND || IMPI || AUTN.

[0047] Como mencionado acima, o primeiro parâmetro pode incluir ou ser derivado de um conjunto de chaves criptográficas. Particularmente, este conjunto de chaves criptográficas pode incluir uma Chave de Cifra (CK) e uma Chave de Integridade (IK) que foram computadas pela entidade de comunicações como parte da operação de segurança. Alternativamente, o conjunto de chaves criptográficas pode ser derivado da Chave de Cifra e da Chave de Integridade.

[0048] Como uma implementação particular, o primeiro parâmetro pode incluir ou ser derivado de uma concatenação de CK e IK, que pode ser expresso como:

CK || IK.

[0049] O dispositivo pode gerar não só a chave criptográfica baseada no primeiro e segundo parâmetros providos, mas também mais chaves criptográficas baseadas na chave criptográfica gerada. Fazendo assim, o dispositivo pode ser adaptado para aplicar uma ou mais funções de derivação de chave adicionais para gerar mais chaves criptográficas baseadas na chave criptográfica sendo gerada.

[0050] Estas "mais chaves criptográficas" podem incluir pelo menos

uma de um conjunto de chaves criptográficas para a proteção de tráfego de Camada Sem Acesso (NAS), um conjunto de chaves criptográficas para a proteção de tráfego de Controle de Recurso de Rádio (RRC), um conjunto de chaves criptográficas para a proteção de tráfego de Plano de Usuário (UP), e uma chave criptográfica intermediária $K_{eNB}$ para derivar as chaves criptográficas para a proteção de tráfego de RRC e/ou as chaves criptográficas para a proteção de tráfego de UP.

[0051] A entidade de comunicações referida acima pode ser um equipamento de usuário, tal como uma estação móvel (por exemplo, um telefone móvel ou um cartão de rede).

[0052] De acordo com um aspecto adicional, um equipamento de usuário incluindo o dispositivo apresentado acima é provido. O equipamento de usuário pode ser uma estação móvel.

[0053] De acordo com ainda um aspecto adicional, um sistema incluindo o equipamento de usuário mencionado acima é provido. O sistema também inclui uma entidade de rede. A entidade de rede pode ser usada dentro de uma rede de SAE/LTE. A entidade de rede pode incluir um AuC/HSS e uma MME. A MME pode ser responsável para iniciar a operação de segurança para o equipamento de usuário. O AuC/HSS pode gerar a chave criptográfica. As chaves criptográficas geradas podem ser compartilhadas pelo equipamento de usuário e a MME. O AuC/HSS pode incrementar o SQN, particularmente cada vez que a operação de segurança é iniciada para o equipamento de usuário. Adicionalmente, o AuC/HSS também pode construir o AUTN baseado no SQN.

Descrição Breve dos Desenhos

[0054] No seguinte, a técnica de geração de chave criptográfica será descrita com referência a concretizações exemplares ilustradas nos desenhos, em que:

Figura 1 é um diagrama mostrando o conceito básico do

protocolo de UMTS AKA;

Figura 2 é um diagrama de bloco ilustrando uma hierarquia de chave proposta para sistema de SAE/LTE;

Figura 3 é um diagrama de bloco mostrando uma concretização de dispositivo;

Figura 4 é um diagrama de bloco mostrando uma concretização de sistema;

Figura 5 é um diagrama de bloco mostrando uma concretização de método;

Figura 6 é um diagrama de bloco mostrando um procedimento da operação de UMTS AKA, Geração de um Vetor de Autenticação por uma entidade de rede;

Figura 7 é um diagrama de bloco mostrando outro procedimento da operação de UMTS AKA, Autenticação e Estabelecimento de Chave;

Figura 8 é um diagrama de bloco mostrando a função de autenticação geral executada pelo UE como parte da operação de UMTS AKA;

Figura 9 é um diagrama de bloco mostrando um algoritmo criptográfico particular para executar a função de autenticação anterior no UE; e

Figura 10 é um diagrama de bloco mostrando um detalhe particular do algoritmo criptográfico anterior.

Descrição Detalhada

[0055] Na descrição seguinte, para propósitos de explicação e não limitação, detalhes específicos estão publicados, tais como seqüências particulares de etapas, interfaces e configurações, a fim de prover uma compreensão completa da técnica de geração de chave criptográfica. Será aparente àqueles qualificados na técnica que a técnica pode ser praticada em

outras concretizações que partem destes detalhes específicos. Por exemplo, enquanto a técnica será descrita principalmente no contexto com o protocolo de UMTS AKA e no ambiente de rede de SAE/LTE, será aparente à pessoa qualificada que a técnica também pode ser praticada com relação a outros protocolos de segurança, arquiteturas, ou ambientes.

[0056] Além disso, aqueles qualificados na técnica apreciarão que as funções explicadas aqui abaixo podem ser implementadas usando software funcionando junto com um microprocessador programado ou computador de propósito geral. Também será apreciado que enquanto a técnica é descrita principalmente na forma de métodos e dispositivos, a técnica também pode ser embutida em um produto de programa de computador como também em um sistema incluindo um processador de computador e uma memória acoplada ao processador, em que a memória é codificada com um ou mais programas que podem executar a função exposta aqui.

[0057] Figura 3 mostra uma concretização de um dispositivo 100 adaptado para gerar uma chave criptográfica para uma entidade de comunicações (não mostrada na Figura 3). A entidade de comunicações é adaptada para correr uma operação de segurança. O dispositivo 100 inclui um primeiro componente 102 e um segundo componente 104. O primeiro componente 102 é adaptado para prover pelo menos dois parâmetros, figurativamente mostrados nas setas 106 e 108.

[0058] O primeiro parâmetro 106 inclui ou é derivado de um conjunto de chaves criptográficas 110 e 112. (Embora duas chaves sejam mostradas na figura, o conjunto de chaves criptográficas pode incluir qualquer número de chaves.) O conjunto de chaves criptográficas foi computado pela entidade de comunicações correndo a operação de segurança. A derivação do conjunto de chaves criptográficas 110 e 112 no primeiro parâmetro 106 é figurativamente mostrada como um bloco 114. O segundo parâmetro 108 inclui ou é derivado de um passe 116. O passe 116 tem um valor diferente cada vez que a operação

de segurança é iniciada para a entidade de comunicações. A derivação do passe 116 no segundo parâmetro 108 é figurativamente mostrada como um bloco 118. O segundo componente 104 do dispositivo 100 é adaptado para correr uma função de derivação chave para gerar uma chave criptográfica 120 baseada no parâmetros providos 106 e 108.

[0059] Se referindo à Figura 4, uma concretização de um sistema 200 incluindo o dispositivo 100 mencionado acima é mostrada. O dispositivo 100 pode ser incluído em uma entidade de comunicações 202, que pode ser um UE, tal como uma estação móvel. Certamente, a entidade de comunicações 202 pode ser qualquer tipo satisfatório de entidade de comunicações capaz de acomodar o dispositivo 100. Adicionalmente, o sistema inclui uma entidade de rede 204, que pode residir em uma rede de SAE/LTE. A entidade de rede 204 pode incluir um AuC ou HSS e uma MME. Também pode ser outra entidade de comunicações em uma rede de SAE/LTE.

[0060] Correspondendo ao dispositivo de geração de chave criptográfica 100 mostrado nas Figuras 3 e 4, um diagrama 300 ilustrando uma concretização de um método para gerar uma chave criptográfica é mostrado na Figura 5. A chave gerada é usada para proteger a comunicação entre duas entidades. A primeira entidade 302 pode corresponder à entidade de comunicações 202 como mostrado na Figura 4, e a segunda entidade 304 pode corresponder à entidade de rede 204 da Figura 4. A primeira entidade pode ser um UE. Porém, a concretização não está limitada a um cenário de entidade de UE-rede. Ao invés, pode ser aplicada a qualquer duas entidades de comunicações em geral.

[0061] A MME pode ser responsável para iniciar a operação de segurança para a entidade de comunicações 202. As chaves criptográficas geradas podem ser compartilhadas pela MME e pela entidade de comunicações 202.

[0062] Particularmente, a concretização de método é executada pela

primeira entidade 302 como parte de uma operação de segurança figurativamente ilustrada na seta 300', que é iniciada pela segunda entidade 304 (particularmente pela MME disso) para a primeira entidade 302. A própria concretização inclui duas etapas, 306 e 308. Etapa 306 provê pelo menos dois parâmetros (106 e 108 da Figura 3). O primeiro parâmetro inclui ou é derivado de um conjunto de chaves criptográficas (110 e 112 como mostrado na Figura 3) que foram computadas pela primeira entidade 302 correndo a operação de segurança 300'. O segundo parâmetro inclui ou é derivado de um passe (116 como mostrado na Figura 3) que tem um valor diferente cada vez que a operação de segurança 300' é iniciada pela segunda entidade 304 para a primeira entidade 302. Na segunda etapa 308, uma função de derivação de chave é aplicada para gerar uma chave criptográfica (120 como mostrado na Figura 3) baseada nos parâmetros providos (106 e 108 como mostrado na Figura 3).

[0063] Abaixo, detalhes significativos são dados para explicar a técnica de geração de chave criptográfica com uma ênfase particular sobre como a técnica pode evitar com êxito as colisões de chave entre dois UEs, ou mais importantemente, entre duas execuções distintas da operação de segurança para um e o mesmo UE.

[0064] A geração de chave criptográfica pode fazer parte da operação de UMTS AKA. O UMTS AKA está baseado na implementação que o UE, particularmente o USIM disso, e o AuC/HSS no Ambiente Doméstico do UE (HE) compartilham uma chave secreta específica de usuário K, certas funções de autenticação de mensagem f1, f2 e certas funções de geração de chave criptográfica f3, f4, f5. Além disso, o USIM e o AuC/HSS mantêm rastro de contadores, ou números de seqüência $SQN_{UE}$ e $SQN_{HE}$ respectivamente para apoiar autenticação de rede. Por exemplo, o AuC/HSS pode incrementar o $SQN_{HE}$, particularmente cada vez que a operação de segurança é iniciada para a primeira entidade. A operação de UMTS AKA inclui vários procedimentos,

incluindo Geração de Vetores de Autenticação (AV), e Autenticação e Estabelecimento de Chave.

[0065] O propósito do procedimento de AV é prover o SN/VLR (ou MME) com um arranjo de AVs novos do HE do UE para executar várias autenticações de usuário. Geração de Vetores de Autenticação pelo HE é ilustrada na Figura 6. Se referindo a esta figura, na recepção de um pedido do SN/VLR, o AuC/HSS envia um arranjo ordenado de n Vetores de Autenticação AV (1...n) para o SN/VLR. Cada AV inclui um número aleatório (ou intimação aleatória) RAND, uma resposta esperada XRES, uma chave de cifra CK, uma chave de integridade IK e um passe de autenticação AUTN.

[0066] O AuC/HSS começa com gerar um novo número de seqüência SQN e uma intimação imprevisível RAND. Subseqüentemente, os valores seguintes são computados:

- um código de autenticação de mensagem MAC = f1(SQN || RAND || AMF), onde f1 é uma função de autenticação de mensagem;

- uma resposta esperada XRES = f2 (RAND), onde f2 é uma função de autenticação de mensagem (possivelmente truncada);

- uma chave de cifra CK = f3 (RAND), onde f3 é uma função geradora de chave;

- uma chave de integridade IK = f4 (RAND), onde f4 é uma função geradora de chave; e

- uma chave de anonimato AK = f5 (RAND), onde f5 é uma função geradora de chave.

[0067] Finalmente, o passe de autenticação AUTN = (SQN xOR AK) || AMF || MAC é construído. Pode ser construído pelo AuC/HSS. Aqui, AK é uma chave de anonimato usada para ocultar o SQN como o anterior pode expor a identidade e localização do UE. A ocultação do SQN é para proteger contra ataques passivos. Uso de AK pode ser opcional. Quando AK

não é usada, o valor AK = 000... 0 pode figurativamente ser usado ao invés.

[0068] O arranjo de AVs é enviado de volta ao SN/VLR pedinte em uma resposta de autenticação. Cada AV é válido para uma (e só uma) autenticação e acordo de chave entre o SN/VLR e o USIM.

[0069] O próximo procedimento da operação de UMTS AKA, Autenticação e Estabelecimento Chave, é autenticar mutuamente e estabelecer novas chaves de cifra e integridade entre o SN/VLR e o UE. Este processo é ilustrado na Figura 7. Se referindo a esta figura, quando o SN/VLR inicia uma autenticação e acordo de chave, seleciona o próximo AV do arranjo e envia os parâmetros RAND e AUTN ao UE. O USIM verifica se AUTN pode ser aceito e, nesse caso, produz uma resposta RES que é enviada de volta ao SN/VLR. Particularmente, os procedimentos do UE são mostrados na Figura 8.

[0070] Se referindo à Figura 8, na recepção de RAND e AUTN, o UE primeiro computa a chave de anonimato AK = f5 (RAND) (ou usa o AK = 000... 0) e recobra o número de seqüência SQN = (SQN xOR AK) xOR AK. A seguir, o UE computa XMAC = f1 (SQN || RAND || AMF) e compara isto com MAC que está incluído em AUTN. Se eles forem diferentes, o UE envia rejeição de autenticação de usuário de volta ao SN/VLR com uma indicação da causa e o UE abandona o procedimento. Se não, o UE verifica que o SQN recebido está na gama correta.

[0071] Se o SQN for considerado estar na gama correta, o UE computa RES = f2 (RAND) e inclui este parâmetro em uma resposta de autenticação de usuário de volta para o SN/VLR. Finalmente, o UE computa a chave de cifra CK = f3 (RAND) e a chave de integridade IK = f4 (RAND). Para melhorar eficiência, RES, CK e IK também poderiam ser computadas mais cedo a qualquer hora depois de receber RAND. O UE pode armazenar RAND para propósitos de re-sincronização.

[0072] Na recepção de resposta de autenticação de usuário, o

SN/VLR compara RES com a resposta esperada XRES do vetor de autenticação selecionado. Se XRES igualar RES, então a autenticação do usuário foi aceita. As chaves computadas recentemente CK e IK então serão transferidas pelo USIM e o SN/VLR às entidades que executam funções de cálculo e integridade.

[0073] Do anterior, pode ser visto que a operação de UMTS AKA está baseada em um par (RAND, AUTN) e AUTN inclui ou é derivado de um número de seqüência, SQN, como:

$$AUTN = (SQN \text{ xOR } AK) \,||\, AMF \,||\, MAC$$

onde o AK é uma chave de anonimato, que pode ser produzida por Milenage (veja Figura 9) de saída "f5" acima.

[0074] A função abaixo é uma primeira solução para o problema de colisão mostrado acima:

$$KDF(CK \,||\, IK, RAND \,||\, IMPI \,||\, SQN)$$

onde SQN assim foi incluído nas entradas. Agora, até mesmo se dois RANDs forem os mesmos, isto é, RAND = RAND', o fato que SQN sempre aumenta (por exemplo, por um) assegurará que entradas são diferentes, únicas, ou distintas.

[0075] Uma solução alternativa é usar:

$$KDF(CK \,||\, IK, RAND \,||\, IMPI \,||\, AUTN).$$

[0076] Esta solução pode ser mais simples para implementar desde que AUTN pode ser usado "como é" da sinalização de AKA. Porém, a "singularidade" das entradas neste caso pode não ser óbvio desde que:

$$AUTN = (SQN \text{ xOR } AK) \,||\, AMF \,||\, MAC$$

e até mesmo se SQN ≠ SQN, não pode ser visto imediatamente que (SQN xOR AK), (SQN' xOR AK') será distinto como AK poderia potencialmente "cancelar" as diferenças. Porém, abaixo, a distinção de (SQN xOR AK) pode ser provada.

[0077] Suponha que:

(CK || IK, RAND || IMPI || AUTN) = (CK' || IK', RAND' || IMPI || AUTN').

[0078] Foi mostrado já que isto implica CK = CK', IK = IK', e RAND = RAND'. Permanece assim ser verificado se poderia ser que AUTN = AUTN'. Esta verificação pode ser traduzida em verificar se:

(SQN xOR AK) || AMF || MAC = (SQN' xOR AK' || AMF' || MAC'.

[0079] Assuma sem perda de generalidade que AMF = AMF' e MAC = MAC'. Então, só é necessário verificar se o seguinte poderia se manter:

SQN xOR AK = SQN' xOR AK'.

[0080] Lembrar que é esperado que RAND = RAND'. Se referindo ao algoritmo de Milenage mostrado na Figura 9, isto implica que AK = AK' (como eles foram produzidos dos mesmos RANDs). Assim, tinha que ser que:

SQN = SQN',

que é uma contradição desde que, como já notado, SQN sempre "cresce" e assim SQN ≠ SQN'.

[0081] Assim, está provado que a segunda solução também garante a singularidade de entradas à função de KDF.

[0082] Como uma solução geral, em vez de usar SQN ou AUTN para alcançar a singularidade, qualquer passe tendo um valor diferente cada vez que a operação de UMTS AKA é iniciada pela rede para o UE é possível. Por exemplo, SQN xOR AK (fazendo parte de AUTN) pode ser usado desde que (pela análise anterior) tem a propriedade de singularidade exigida.

[0083] A técnica de geração de chave criptográfica descrita aqui acima apresenta numerosas vantagens. Por exemplo, garante singularidade de entradas de KDF. Conseqüentemente, evita com êxito as comissões provocadas por possíveis entradas idênticas. Com esta técnica, a chave criptográfica gerada deverá ser capaz de satisfazer, por exemplo, as exigências de segurança de alto nível em sistemas de SAE/LTE. Como uma

vantagem adicional, a técnica pode ser implementada baseada em USIMs já desdobrados sem requerer qualquer substituição de USIM. Outra vantagem específica com usar AUTN em lugar de SQN é que a invenção pode ser implementada no término móvel (fora do USIM).

[0084] Embora concretizações da técnica de geração de chave criptográfica tenham sido ilustradas nos desenhos acompanhantes e descritas em uma descrição precedente, será entendido que a técnica não está limitada às concretizações expostas aqui. A técnica é capaz de numerosos rearranjos, modificações e substituições sem partir da extensão da invenção.

REIVINDICAÇÕES

1. Método para gerar uma chave criptográfica (120) para proteger comunicação entre duas entidades (202, 204), em que o método é executado pela primeira entidade (202, 302) como parte de um procedimento de Autenticação e Acordo de Chave <AKA> com base em um protocolo AKA UMTS iniciado pela segunda entidade (204, 304), o método caracterizado pelo fato de que compreende as etapas de:

prover (306) pelo menos dois parâmetros (106, 108), em que o primeiro parâmetro (106) inclui ou é derivado de um conjunto de chaves criptográficas (110, 112) tendo sido computadas pela primeira entidade (202) executando o procedimento AKA, e o segundo parâmetro inclui ou é derivado de um passe (116) tendo um valor diferente cada vez que o procedimento AKA é iniciada pela segunda entidade (204, 304) para a primeira entidade (202, 302); e

aplicar (308) uma função de derivação de chave para gerar uma chave criptográfica (120) baseada nos parâmetros providos (106, 108);

em que o passe (116) é uma concatenação do OU exclusivo de um número de sequência <SQN> e uma Chave de Anonimato <AK>, um Campo de Autenticação e Administração de Chave <AMF>, e um Código de Autenticação de Mensagem <MAC>,

em que o <SQN> indica o número de vezes que o procedimento AKA foi iniciado pela segunda entidade (204, 304) para a primeira entidade (202, 302), e

em que a AK é uma chave criptográfica produzida por uma função de geração de chave f5 usando uma intimação aleatório de acordo com o protocolo AKA UMTS.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o conjunto de chaves criptográficas (110, 112) incluído no primeiro parâmetro (106) ou de qual o primeiro parâmetro (106) é derivado

inclui ou é derivado de uma Chave de Cifra <CK> (110) e uma Chave de Integridade <IK> (112).

3. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que adicionalmente inclui a etapa de:

aplicar uma ou mais funções de derivação de chave adicionais para gerar mais chaves criptográficas baseadas na chave criptográfica (120) gerada.

4. Método de acordo com a reivindicação 3, caracterizado pelo fato de que as mais chaves criptográficas incluem pelo menos um do seguinte:

um conjunto de chaves criptográficas para a proteção de tráfego de Camada Sem Acesso <NAS>;

um conjunto de chaves criptográficas para a proteção de tráfego de Controle de Recurso de Rádio <RRC>;

um conjunto de chaves criptográficas para a proteção de tráfego de Plano de Usuário <UP>; e

uma chave criptográfica intermediária <KeNB> para derivar as chaves criptográficas para a proteção de tráfego de RRC e/ou as chaves criptográficas para a proteção de tráfego de UP.

5. Método de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que a primeira entidade (202, 302) é um equipamento de usuário.

6. Método de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que a segunda entidade (204, 304) é uma entidade de rede.

7. Método de acordo com a reivindicação 6, caracterizado pelo fato de que a segunda entidade (204, 304) reside em uma rede de Evolução de Arquitetura de Sistema <SAE>/Evolução de Longo Prazo <LTE>.

8. Método de acordo com a reivindicação 6 ou 7, caracterizado pelo fato de que a segunda entidade (204, 304) inclui um Centro de

Autenticação <AuC/Servidor de Assinante Doméstico <HSS> e uma Entidade de Administração de Mobilidade <MME>.

9. Método de acordo com qualquer uma das reivindicações 1 a 8, caracterizado pelo fato de que o procedimento de Autenticação e Acordo de Chave é executado cooperativamente pela primeira (202, 302) e segunda (204, 304) entidades.

10. Meio de armazenamento legível por computador, caracterizado pelo fato de que compreende instruções legíveis por computador que, quando lidas por um computador, fazem com que o mesmo realize o método conforme definido em qualquer uma das reivindicações 1 a 9.

11. Dispositivo (100) adaptado para gerar uma chave criptográfica (120) para uma entidade de comunicações (202, 302) adaptada para executar um procedimento de Autenticação e Acordo de Chave <AKA> com base em um protocolo AKA UMTS, o dispositivo (100) caracterizado pelo fato de que inclui:

um primeiro componente (102) adaptado para prover pelo menos dois parâmetros (106, 108), em que o primeiro parâmetro (106) inclui ou é derivado de um conjunto de chaves criptográficas (110, 112) tendo sido computadas pela entidade de comunicações (202, 302) móvel executando o procedimento AKA, e o segundo parâmetro (108) inclui ou é derivado de um passe (116), os pelo menos dois parâmetros providos tendo um valor diferente cada vez que o procedimento AKA é iniciada para a entidade de comunicações (202, 302) móvel; e

um segundo componente (104) adaptado para executar uma função de derivação chave para gerar uma chave criptográfica (120) baseada nos parâmetros providos (106, 108);

em que o passe (116) inclui uma concatenação do OU exclusivo de um número de sequência <SQN> e uma Chave de Anonimato (AK), um Campo de Autenticação e Administração de Chave <AMF>, e um

Código de Autenticação de Mensagem <MAC>,

em que o <SQN> indica o número de vezes que o procedimento AKA iniciada para a entidade de comunicações (202, 302) móvel, e

em que a AK é uma chave criptográfica produzida por uma função de geração de chave f5 usando uma intimação aleatória de acordo com o protocolo AKA UMTS.

12. Dispositivo (100) de acordo com a reivindicação 11, caracterizado pelo fato de que o conjunto de chaves criptográficas (110, 112) incluído no primeiro parâmetro (106) ou de qual o primeiro parâmetro (106) é derivado inclui ou é derivado de uma Chave de Cifra <CK> (110) e uma Chave de Integridade <IK> (112) computadas pela entidade de comunicações (202, 302) como parte da procedimento de Autenticação e Acordo de Chave.

13. Dispositivo (100) de acordo com a reivindicação 11 ou 12, caracterizado pelo fato de ser adicionalmente adaptado para aplicar uma ou mais funções de derivação de chave adicionais para gerar mais chaves criptográficas baseadas na chave criptográfica (120) gerada.

14. Equipamento de usuário (202), caracterizado pelo fato de que inclui o dispositivo (100) como definido em qualquer uma das reivindicações 11 a 13.

15. Sistema, caracterizado pelo fato de que inclui o equipamento de usuário (202, 302) como definido na reivindicação 14 e uma entidade de rede (304).

16. Sistema de acordo com a reivindicação 15, caracterizado pelo fato de que a entidade de rede (304) é para uso em uma rede de SAE/LTE.

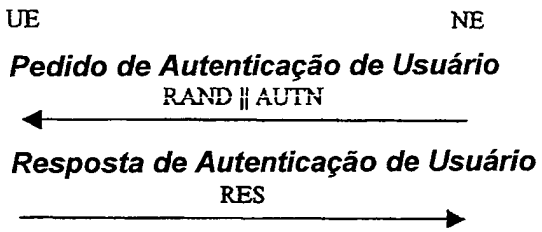
UE
NE
Pedido de Autenticação de Usuário
RAND || AUTN
Resposta de Autenticação de Usuário
RES

Fig. 1

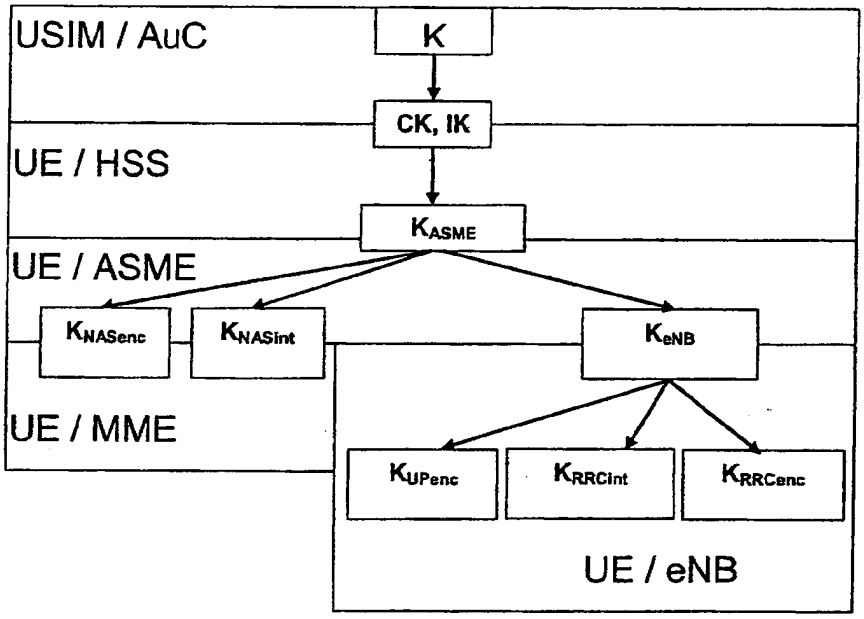
USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / ASME
KNASenc
KNASint
KeNB
UE / MME
KUPenc
KRRCint
KRRCenc
UE / eNB

Fig. 2

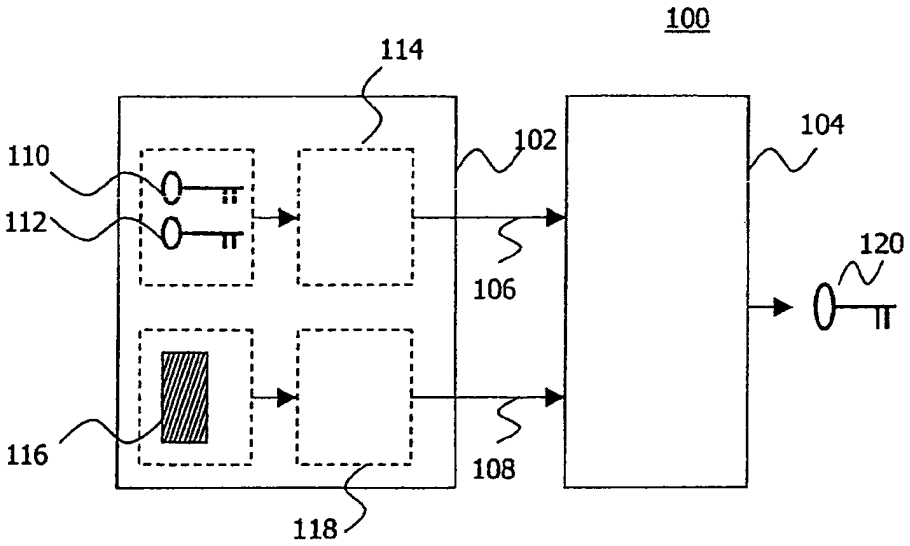


Fig. 3

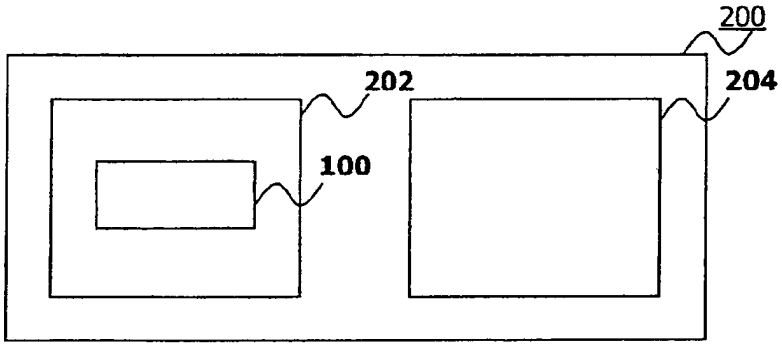


Fig. 4

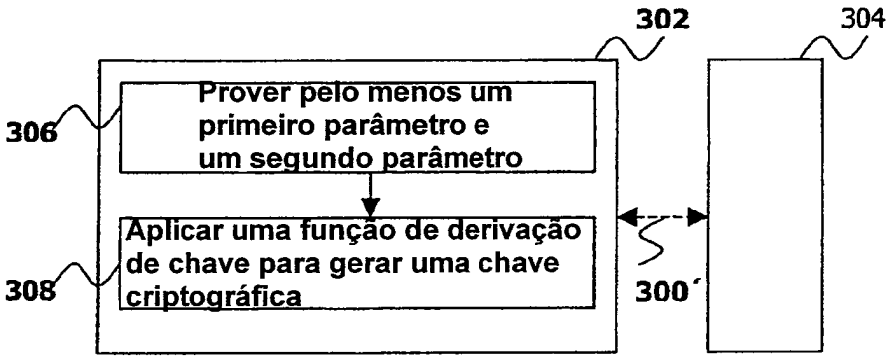


Fig. 5

300

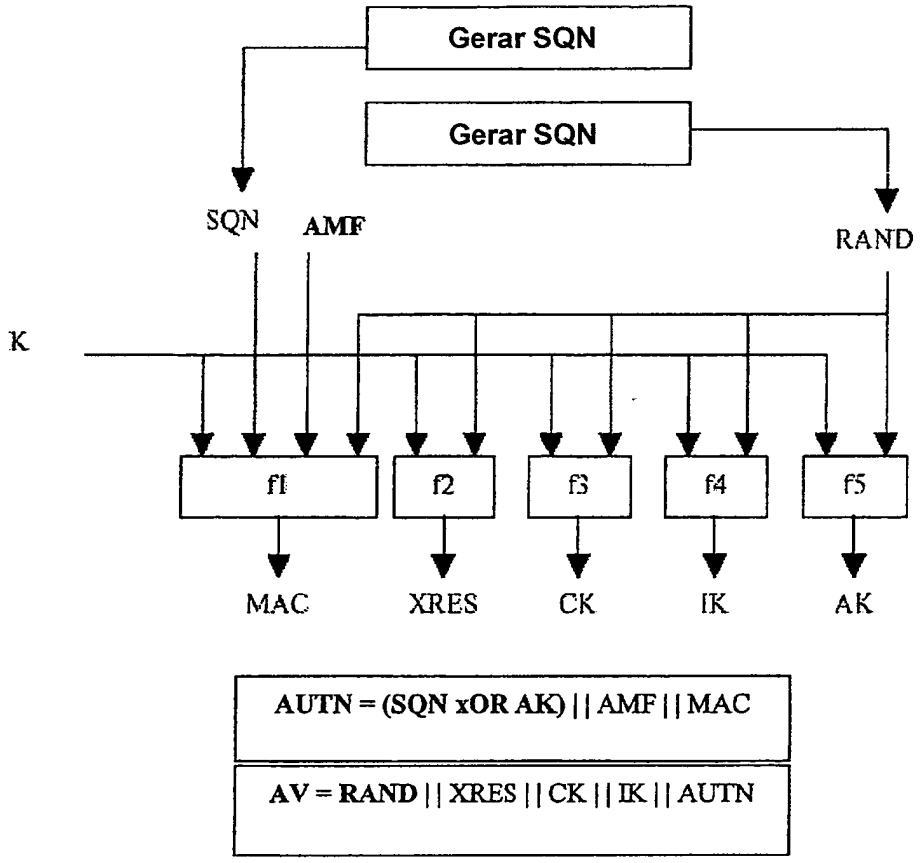
Gerar SQN
Gerar SQN
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN = (SQN xOR AK) || AMF || MAC
AV = RAND || XRES || CK || IK || AUTN

Fig. 6

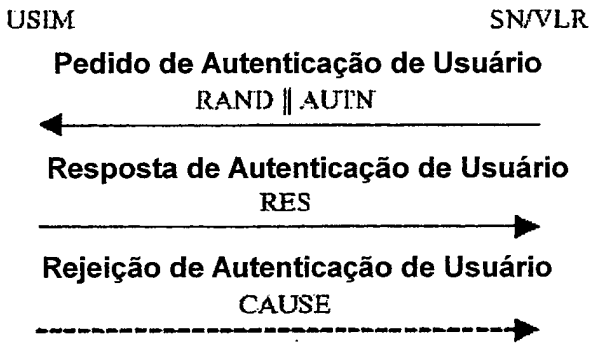
USIM
SN/VLR
Pedido de Autenticação de Usuário
RAND || AUTN
Resposta de Autenticação de Usuário
RES
Rejeição de Autenticação de Usuário
CAUSE

Fig. 7

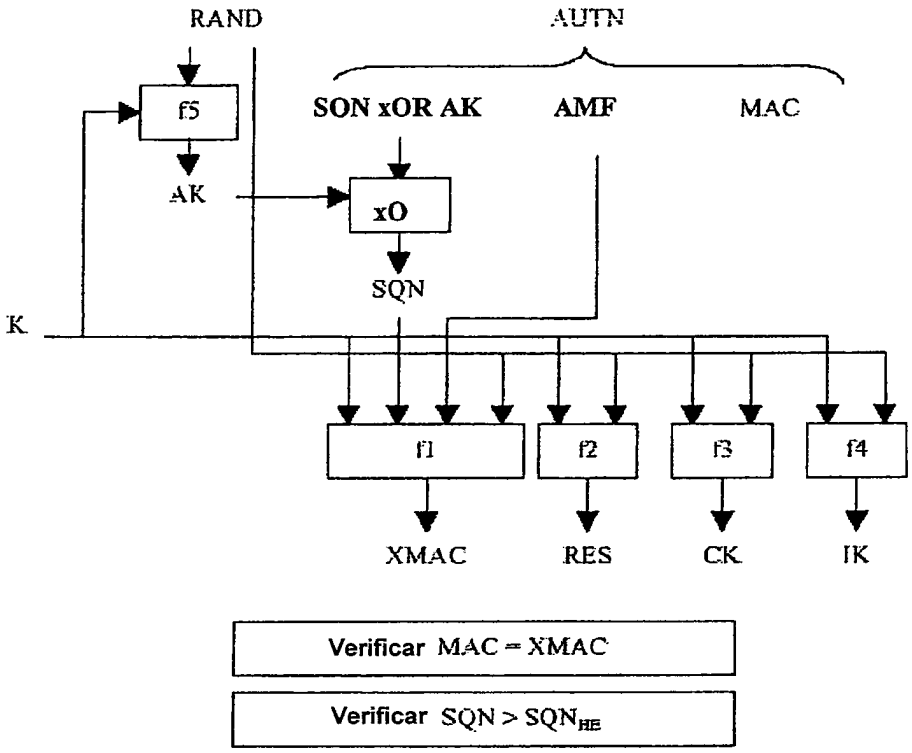
RAND
AUTN
f5
SON xOR AK
AMF
MAC
AK
xO
SQN
K
f1
f2
f3
f4
XMAC
RES
CK
IK
Verificar MAC = XMAC
Verificar SQN > SQN$_{HE}$

Fig. 8

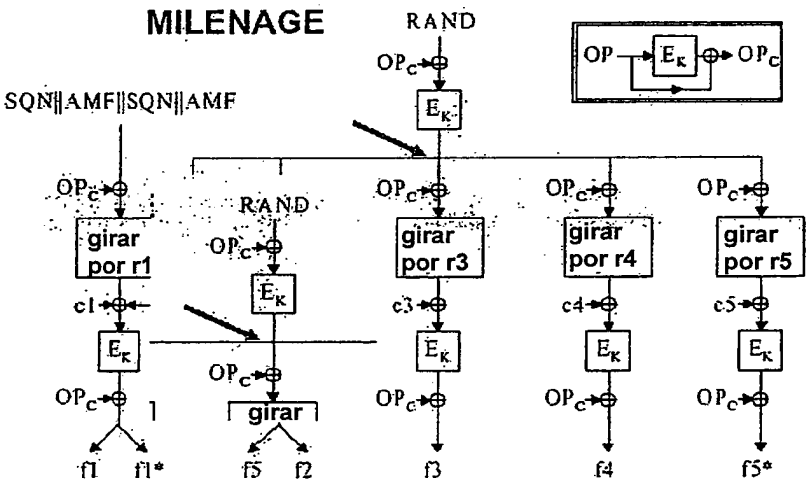
MILENAGE
RAND
OP
$E_K$
$OP_C$
SQN||AMF||SQN||AMF
girar por r1
girar por r3
girar por r4
girar por r5
girar
c1
c3
c4
c5
f1
f1*
f5
f2
f3
f4
f5*

Fig. 9

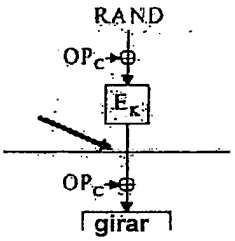
RAND
$OP_C$
$E_K$
girar

Fig. 10