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

(11) **PI 0209755-9 B1**

**(22) Data do Depósito:** 28/05/2002

**(45) Data de Concessão:** 01/12/2015

**(RPI 2343)**

**(54) Título:** MÉTODO E SISTEMA PARA ASSEGURAR UMA TRANSMISSÃO DE DADOS SEGURA ENTRE O PRIMEIRO E O SEGUNDO DISPOSITIVOS DE COMUNICAÇÃO EM UMA COMUNICAÇÃO SEM FIO DE ALCANCE LIMITADO, E, DISPOSITIVO DE COMUNICAÇÃO

**(51) Int.Cl.:** H04L 9/08; H04L 9/32

**(30) Prioridade Unionista:** 08/06/2001 FI 20011215

**(73) Titular(es):** NOKIA CORPORATION

**(72) Inventor(es):** KAISA NYBERG, VALTTERI NIEMI

**"MÉTODO E SISTEMA PARA ASSEGURAR UMA TRANSMISSÃO DE DADOS SEGURA ENTRE O PRIMEIRO E O SEGUNDO DISPOSITIVOS DE COMUNICAÇÃO EM UMA COMUNICAÇÃO SEM FIO DE ALCANCE LIMITADO, E, DISPOSITIVO DE COMUNICAÇÃO".**

Campo da Invenção

A presente invenção relaciona a um método para assegurar uma transmissão de dados segura entre um primeiro e um segundo dispositivo de comunicação em uma comunicação sem fio de alcance limitado na qual, para estabelecer uma conexão de transmissão de dados, os dispositivos de comunicação conduzem a um estágio de troca de chave para trocar ao menos duas chaves entre os dispositivos de comunicação, e com base nas chaves trocadas ao menos uma chave de codificação é derivada dos dispositivos de comunicação. A invenção também relaciona a um sistema de comunicação que inclui ao menos o primeiro e o segundo dispositivo de comunicação, um dispositivo para estabelecer uma conexão de transmissão de dados sem fio de alcance limitado entre o primeiro e o segundo dispositivo de comunicação e um dispositivo para assegurar uma transmissão de dados segura na conexão de transmissão de dados, incluindo um dispositivo para conduzir um estágio de troca de chave para trocar ao menos duas chaves entre os dispositivos de comunicação, e um dispositivo para derivar ao menos uma chave de codificação com base nas chaves trocadas nos dispositivos de comunicação. Em adição, a invenção relaciona a um dispositivo de comunicação que inclui ao menos um dispositivo para estabelecer uma conexão de transmissão de dados sem fio de alcance limitado entre o dispositivo de comunicação e o outro dispositivo de comunicação e um dispositivo para assegurar uma transmissão de dados segura na conexão de transmissão de dados, incluindo um dispositivo para conduzir o estágio de troca de chave com outro dispositivo de comunicação para trocar ao menos duas chaves entre os dispositivos de comunicação, e um dispositivo para derivar ao menos uma chave de codificação com base nas chaves trocadas.

Descrição da Técnica Anterior

Nesta especificação, o conceito de conexão de transmissão de dados sem fio de alcance limitado recorre principalmente a tais conexões, nas quais dois ou mais dispositivos que são localizados relativamente próximo um do outro podem comunicar entre

si de uma maneira sem fio. Na comunicação é possível aplicar, por exemplo, comunicação de rádio, comunicação infravermelha, comunicação indutiva, ou similar. Por exemplo, a tecnologia Bluetooth™, na qual os transmissores de rádio de baixa-potência e os receptores de rádio são usados, tem sido desenvolvido com a finalidade de comunicação de rádio de alcance limitado. Tais dispositivos podem comunicar entre si e assim formam um sistema de comunicação ad hoc. Ao aplicar a tecnologia de comunicação de alcance limitado é, por exemplo, possível conectar os dispositivos periféricos a um computador de maneira sem fio. Além disso, por exemplo, o dispositivo de comunicação sem fio pode ser acoplado a um computador portátil, onde do computador é possível ter uma conexão sem fio a outra rede de comunicação, tal como a rede de dados Internet. Assim, uma situação pode ocorrer na qual, o usuário tem que entrar com a identificação de usuário dele e a senha quando ele/ela estiver estabelecendo uma conexão com a rede de dados por meio do computador portátil. Assim, há um risco que é possível espiar a identificação do usuário e a senha transmitida sem codificação entre o computador portátil e o dispositivo de comunicação sem fio conectado neste com uma conexão sem fio de alcance limitado.

Outras possíveis áreas de implementação para conexões de transmissão de dados de alcance limitado que podem ser mencionadas neste contexto incluem a rede de área local sem fio (WLAN), o sistema terminal de pagamento sem fio e a fechadura operacional sem fio. Por meio da rede de área local sem fio, por exemplo, quando instalada em um escritório pequeno é possível implementar uma rede de área local que inclui vários computadores sem ter que conduzir o cabeamento. No sistema terminal de pagamento sem fio, o usuário pode pagar a fatura, por exemplo, por meio de um dispositivo de comunicação sem fio, que também contém dispositivos de comunicação de alcance limitado. Assim, uma conexão de transmissão de dados de alcance limitado é estabelecida entre o dispositivo de comunicação sem fio e o terminal de pagamento com a finalidade de pagamento das contas. Correspondentemente, em uma fechadura operacional sem fio, o usuário tem uma chave que comunica sem fio com a fechadura, para assegurar que a chave em questão seja planejada para controlar a função desta fechadura em particular. Tal chave pode ser implementada como uma chave separada, ou pode ser implementada com relação a outro dispositivo, tal como um dispositivo de comunicação sem fio.

Em tais sistemas de comunicação é problemático como as partes diferentes na comunicação podem estar seguras de que os dispositivos em questão estão realmente autorizados ao processo de comunicação. Isto é especialmente importante em tais situações, onde a informação confidencial é transferida entre os diferentes dispositivos. Por exemplo, na incorporação acima mencionada do terminal de pagamento, o terminal de pagamento tem que assegurar que o dispositivo realmente usado na transação de pagamento seja o dispositivo usado pelo proprietário de conta em questão ou uma pessoa autorizada pelo proprietário da conta. Também na incorporação da fechadura, a fechadura tem que assegurar a autenticidade da chave antes da fechadura ser aberta. Em tais incorporações, com a finalidade de verificar as partes, a comunicação entre os dispositivos tem que ser protegida, de possíveis intrusos externos, tal como os intrometidos e partes intervenientes. De forma a levar em conta estes aspectos de segurança, foram desenvolvidos mecanismos de codificação diferentes, por exemplo, para os sistemas Bluetooth™. As técnicas que são usadas incluem, por exemplo, um par de chaves (PKI, Infraestrutura de Chave Pública) composto de uma chave pública e uma chave privada. Em tal arranjo, o usuário tem uma chave pública que ele pode enviar uma contra-parte sem codificação, e uma chave privada que não tem que ser transferida para o sistema de comunicação em nenhum estágio, mas o usuário tem que manter esta escondida. Assim, é possível transmitir a informação codificada ao usuário, codificando a informação com a chave pública. O usuário pode decifrar a informação com a sua chave privada.

Uma desvantagem do sistema de codificação assimétrico do tipo acima é que é relativamente lento, onde a codificação de grandes quantidades de informação desacelera consideravelmente a transmissão de dados. Os sistemas de comunicação também aplicam métodos de codificação simétricos, nos quais ambas as partes da comunicação compartilham a mesma chave privada (chave compartilhada, secreta compartilhada). Um problema nesta disposição é, por exemplo, como esta chave privada pode ser transmitida para outro dispositivo, de forma que um estranho não possa descobrir a chave privada. Em alguns casos o próprio usuário pode entrar com esta chave privada para diferentes dispositivos. No dispositivo de acordo com o sistema Bluetooth™, esta chave privada é utilizada para calcular uma chave de enlace usada na comunicação de rádio, por meio da

qual a chave de enlace da informação atual a ser transmitida é codificada. O comprimento máximo determinado para a chave de enlace é de 128 bits, onde o comprimento da chave privada deveria ser pelo menos de 32 caracteres. É laborioso entrar com tal cadeia de caracteres contendo 32 caracteres, e há alta probabilidade de erros, especialmente quando a cadeia de caracteres tem que ser entrada sucessivamente pelo menos duas vezes sem erros antes da conexão poder ser estabelecida.

A patente US 5,241,599 descreve um método para troca da chave codificada (TCC), na qual a chave de codificação usada na comunicação é codificada primeiro com uma chave de codificação curta, logo após a chave de codificação pode ser transmitida no formato codificado de um dispositivo para outro, através do canal de comunicação não codificado. Nos sistemas de alcance limitado este método pode ser aplicado, de tal maneira que o usuário entra com a chave de codificação curta em ambos os dispositivos, logo após ambos os dispositivos transmitem a chave de codificação deles próprios para outro dispositivo, codificada com uma chave de codificação curta. Tais sistemas têm a desvantagem, por exemplo, de que a eficiência de codificação é, por exemplo, dependente de com que freqüência o usuário muda esta chave de codificação curta. Além disso, tal chave de codificação curta selecionada pelo usuário pode ser adivinhada de forma relativamente fácil, e então quando o método for aplicado, é possível que os estranhos descubram a chave de codificação curta.

Há o método denominado de Diffie-Hellman conhecido que é baseado no módulo de exponenciação de um número primo grande. Com base nisto, a dificuldade na quebra da codificação implementada com o método de Diffie-Hellman é considerada hoje diretamente proporcional à dificuldade de calcular o módulo de logaritmos discretos de um número primo grande. O método de Diffie-Hellman é uma chave pública baseada no algoritmo geralmente usado especialmente na troca de chave. O método é considerado seguro quando as chaves de comprimento suficiente e um gerador DH apropriado são usados. No método de Diffie-Hellman, a primeira parte determina o primeiro número da chave com base no primeiro número secreto e o primeiro número de chave é transmitido para a segunda parte. Correspondentemente, a segunda parte determina o segundo número de chave com base no segundo número secreto e o segundo número de chave é transmitido

para a primeira parte. Depois disso, a primeira parte gera o terceiro número de chave com base no primeiro número secreto e o segundo número de chave recebido, e a segunda parte gera um quarto número de chave com base no segundo número secreto e no primeiro número de chave recebido. O terceiro e o quarto números de chave são idênticos, e eles não são transmitidos entre as partes envolvidas. O terceiro e o quarto números de chave podem ser usados para a codificação e a decodificação da informação a ser transmitida entre as partes. Neste arranjo é, contudo, possível que uma terceira parte seja capaz de mudar o primeiro número de chave ou o segundo número de chave. Isto ocorre, por exemplo, de tal maneira que a terceira parte se coloca entre a primeira e a segunda parte (MIM, Homem No Meio), onde a primeira parte confunde a terceira parte com a segunda parte, e, de uma maneira correspondente, a segunda parte confunde a terceira parte com a primeira parte. Assim, na prática, os dados são transmitidos entre a primeira e a segunda parte pela terceira parte, e a terceira parte detecta ambas as mensagens transmitidas pela primeira parte e as mensagens transmitidas pela segunda parte, e é capaz de as modificar. O método de Diffie-Hellman é descrito em maiores detalhes na patente US 4,200,770 a qual referência é feita neste contexto.

Uma melhoria foi sugerida para o método de Diffie-Hellman, por meio do qual as diferentes partes no método de comunicação sem fio de alcance limitado podem ser verificadas. O método é descrito na publicação F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks" 1999 AT&T Software Simpósio. O método descrito nesta publicação é baseado no fato de que ambas as partes verificam que o terceiro e o quarto números de codificação obtidos como resultado das ações descritas acima são idênticos. Isto pode ser conduzido, por exemplo, de tal maneira que os números de codificação calculados sejam exibidos nos dispositivos das partes e os usuários dos dispositivos comparem estes números entre si. Porém, para atingir uma codificação suficientemente forte (uma chave de codificação de pelo menos 128 bits), os números de codificação têm que ser cadeias de caracteres compostas de pelo menos 32 caracteres. É difícil de comparar tais cadeias de caracteres que são relativamente longas, e a probabilidade de erro é alta.

Resumo da Invenção

É um objetivo da presente invenção para prover um método melhorado para assegurar uma transmissão de dados segura, um sistema de comunicação e um dispositivo de comunicação. A invenção é baseada na idéia de que uma única cadeia curta de caracteres randômicos é selecionada, com base na qual o código de verificação é calculado em ambos os dispositivos e o código de verificação calculado é apresentado ou em um dispositivo ou em ambos os dispositivos. Se ambos os dispositivos apresentam o código de verificação que eles calcularam, eles podem ser comparados com os códigos entre si. Se apenas um dispositivo apresenta o código de verificação, este é a entrada para o outro dispositivo, no qual o código de verificação de entrada é comparado ao código de verificação calculado no dispositivo. Mais precisamente, o método de acordo com a presente invenção é caracterizado principalmente pelo fato de que no estágio de troca de chave ao menos a primeira e a segunda cadeia de caracteres de verificação são geradas, as cadeias de caracteres de verificação sendo baseadas ao menos nas chaves derivadas no estágio de troca de chave, e onde a segurança da conexão estabelecida é assegurada ao comparar a correspondência das cadeias de caracteres de verificação. O sistema de comunicação de acordo com a presente invenção é caracterizado principalmente pelo fato de que compreende um dispositivo para assegurar uma transmissão de dados segura em uma conexão de transmissão de dados compreendendo um dispositivo para formar ao menos a primeira e a segunda cadeias de caracteres de verificação, que são baseadas ao menos nas chaves derivadas no estágio de troca de chave, e um dispositivo para comparar a correspondência das cadeias de caracteres de verificação. O dispositivo de comunicação de acordo com a presente invenção é caracterizado principalmente pelo fato de que compreende um dispositivo para assegurar uma transmissão de dados segura em uma conexão de transmissão de dados compreendendo um dispositivo para gerar ao menos uma cadeia de caracteres de verificação, que é baseada ao menos nas chaves derivadas no estágio de troca de chave, e no dispositivo a ser usado para comparar a correspondência das cadeias de caracteres de verificação.

A presente invenção apresenta vantagens notáveis comparadas às soluções da técnica anterior. Quando o método de acordo com a invenção for aplicado, é possível verificar as partes envolvidas na comunicação sem ter que usar muito tempo e as chaves de

codificação complexas ou os números de verificação na verificação. Não é necessário o próprio usuário entrar com qualquer número de identificação no início do estabelecimento de uma conexão, mas o estabelecimento de uma conexão normalmente é iniciado ao selecionar, por exemplo, o segundo dispositivo do menu que é formado no dispositivo para este propósito. Considerando que, as cadeias de caracteres de verificação em um tempo são usadas no método de acordo com a invenção, não é fácil de adivinhar as cadeias de caracteres de verificação e, por outro lado, porque a mesma cadeia de caracteres de verificação não é usada da próxima vez que a autenticação for executada, e os estranhos não terão nenhum uso para as cadeias de caracteres de verificação descritas após. Assim, uma melhor segurança do sistema de comunicação é obtida do que quando as soluções da técnica anterior são usadas.

Breve Descrição das Figuras

A seguir a invenção será descrita em maiores detalhes com referência às figuras apensas, nas quais:

Figura 1 – apresenta o método de acordo com a incorporação preferida da invenção em um fluxograma reduzido;

Figura 2 – apresenta o método de acordo com a segunda incorporação preferida da invenção em um modo reduzido;

Figura 3 – apresenta o método de acordo com a terceira incorporação preferida da invenção em um modo reduzido; e

Figura 4 – apresenta um sistema de comunicação de acordo com a incorporação preferida da invenção em um fluxo reduzido.

Descrição Detalhada da Invenção

A seguir, a operação do método de acordo com a incorporação preferida da invenção será descrito em maiores detalhes com referência ao fluxo reduzido apresentado na Figura 1 e usando o sistema de comunicação de acordo com a Figura 4 como um exemplo. Este compreende o primeiro 2 dispositivo de comunicação e o segundo 3 dispositivo de comunicação. O primeiro 2 dispositivo de comunicação é, por exemplo, um computador portátil (PC Laptop). O segundo 3 dispositivo de comunicação é, por exemplo, um dispositivo de comunicação sem fio, tal como o telefone móvel instalado no carro do

usuário. É, contudo, óbvio que estes dispositivos 2, 3 de comunicação sejam apenas exemplos incorporativos não-restritivos, e os dispositivos 2, 3 de comunicação usados em conexão com a invenção podem também diferir destes apresentados aqui. O primeiro 2 e o segundo 3 dispositivos de comunicação compreendem os dispositivos de comunicação local 4a, 4b, tal como o receptor de rádio potência baixa (LPRF, RF de Potência Baixa), um transmissor e receptor infravermelhos, ou similares. Por meio dos dispositivos de comunicação local 4a, 4b, os dispositivos de comunicação podem comunicar entre si de forma sem fio. Em adição, os dispositivos de comunicação 2, 3 contêm os blocos de controle 5a, 5b que vantajosamente compreendem um microprocessador ou similar, e a memória 6a, 6b. O sistema de acordo com a incorporação preferida contém ao menos no primeiro 2 dispositivo de comunicação, o visor 7a , 7b para apresentar a informação e ao menos o segundo 3 dispositivo de comunicação contém o dispositivo de entrada 8b para entrar com a informação para o segundo 3 dispositivo de comunicação. O dispositivo de entrada 8b é vantajosamente um teclado, mas é óbvio que outros tipos de dispositivos de entrada, tal como o dispositivo de entrada de dados baseado no controle de áudio pode ser aplicado neste contexto. O primeiro dispositivo de comunicação 2 pode também conter os dispositivos de entrada 8a, embora eles não sejam necessários neste método de acordo com a incorporação preferida da invenção. Os dispositivos de comunicação 2, 3 podem também compreender os dispositivos de áudio 10a, 10b, tal como o fone de ouvido/alto-falante e/ou um microfone. No sistema de acordo com a Figura 4, o segundo 3 dispositivo de comunicação também compreende as funções da estação móvel, as quais são ilustradas pelo bloco 9.

Na situação onde o objetivo é estabelecer uma conexão de transmissão de dados entre o primeiro e o segundo dispositivos de comunicação, os passos a seguir são obtidos do método de acordo com esta incorporação preferida da invenção. Os dispositivos de comunicação 2, 3 detectam se existem outros dispositivos de comunicação possíveis na vizinhança, para os quais a conexão de transmissão de dados pode ser estabelecida. Neste contexto, este estágio é denominado de estágio de paginação, e este pode ser implementado, por exemplo, da maneira a seguir. Ao menos um dispositivo de comunicação 2, 3 transmite as mensagens de paginação ou similares nos intervalos, e ouve as possíveis mensagens de

resposta por meio do receptor do dispositivo de comunicação local 4. Assim, na situação onde os dispositivos de comunicação 2, 3 transmitem a mensagem de paginação, os dispositivos de comunicação 2, 3 que tem recebido a mensagem de paginação transmitem uma mensagem de resposta para os dispositivos de comunicação 2, 3 que tem transmitido a mensagem de paginação. O usuário do dispositivo de comunicação pode ser apresentado com uma lista de outros dispositivos de comunicação, que são possivelmente detectados na vizinhança. Assim, o usuário pode selecionar um ou mais dispositivos de comunicação desta lista, e a conexão de transmissão de dados é estabelecida para este. Quando o método de acordo com a invenção é aplicado no estabelecimento da conexão de transmissão de dados, este não é, contudo, necessário para o usuário entrar com um número de identificação ou similar. Na conexão com o estágio de paginação, os dispositivos de comunicação 2, 3 podem transmitir os próprios endereços deles para a outra parte envolvida na conexão de transmissão de dados a ser estabelecida, onde estes endereços individualizam os dispositivos de comunicação 2, 3 que são usados na comunicação a seguir. Após o estágio de paginação, ambos os dispositivos de comunicação 2, 3 executam o estágio de troca da chave interativa (seta 102 na Figura 1) para gerar a mesma chave secreta CH em ambos os dispositivos. O estágio de troca da chave é conduzido (seta 102 na Figura 1) usando, por exemplo, o protocolo de troca de chave Diffie-Hellman. Assim, no primeiro dispositivo de comunicação os parâmetros a, q são selecionados, o primeiro número secreto X1 é gerado, e o primeiro número de chave Y1 é calculado vantajosamente por meio da fórmula $Y1 = a^{X1} \bmod q$. O primeiro 2 dispositivo de comunicação transmite os valores numéricos a, q, Y1 para o segundo 3 dispositivo de comunicação. O segundo 3 dispositivo de comunicação gera o segundo número secreto X2, calcula o segundo número da chave por meio da fórmula $Y2=a^{X2} \bmod q$ e transmite o segundo número de chave Y2 para o primeiro dispositivo de comunicação. Após este estágio de troca de chave, a chave de codificação compartilhada CH é calculada em ambos os dispositivos de comunicação 2, 3. O primeiro 2 dispositivo de comunicação utiliza o parâmetro q, o segundo número de chave Y2 e o primeiro número secreto X1, e calcula $CH1 = (Y2)^{X1} \bmod q$. De uma maneira correspondente, o segundo 3 dispositivo de comunicação utiliza o parâmetro q, o primeiro número de chave Y1 e o segundo número secreto X2, e calcula $CH2 = (Y1)^{X2} \bmod q$. Se a transmissão de dados tiver

sido conduzida sem problemas, e estranhos não tiverem influenciado o processo de transmissão de dados, este é verdadeiro para CH1 = CH2, então ambos os dispositivos de comunicação 2, 3 estarão atentos para a mesma chave de codificação compartilhada CH (=CH1=CH2), que pode ser usada para codificação da informação a ser transmitida através da conexão de transmissão de dados e para decodificação após as partes terem verificado a autenticidade de cada outra.

Se a chave de codificação produzida pelo protocolo de troca de chave for mais longa do que o comprimento máximo reservado para a chave de codificação compartilhada CH na aplicação, é possível formar a chave de codificação compartilhada atual CH da chave de codificação produzida no protocolo de troca de chave, por exemplo, ao cortar esta em um comprimento adequado ou ao selecionar as partes predeterminadas desta. Por exemplo, nos sistemas baseado na tecnologia Bluetooth™ atual é possível usar as chaves de codificação com o comprimento máximo de 128 bits como uma chave de codificação compartilhada CH.

Como foi declarado anteriormente nesta descrição, é possível que uma terceira parte tenha tomado parte no processo de troca de chave, sendo então capaz de influenciar a comunicação entre o primeiro 2 e o segundo 3 dispositivos de comunicação, e desse modo tendo a oportunidade de mudar os números de chave transmitidos Y1, Y2. Assim, é possível conduzir o próximo estágio de verificação, no qual o objetivo é detectar se o estágio de troca de chave tem sido conduzido de uma maneira segura. Nesta incorporação preferida da invenção, o primeiro 2 dispositivo de comunicação seleciona uma cadeia de caracteres randômicos única P (bloco 103 na Figura 1), que é relativamente curta, por exemplo, de 6 caracteres longos. Esta seleção pode ser conduzida de maneira conhecida para tal, por exemplo, ao gerar esta usando um gerador de cadeia de caracteres randômicos fornecidos no software de aplicação do bloco de controle. Além de selecionar a cadeia de caracteres randômicos P, o primeiro 2 dispositivo de comunicação calcula a primeira C1 cadeia de caracteres de verificação (bloco 104) com base na cadeia de caracteres randômicos P gerada e na chave de codificação compartilhada CH. O comprimento desta cadeia de caracteres de verificação é preferivelmente igual ao comprimento da cadeia de caracteres randômicos, isto é, nesta situação de exemplo, 6 caracteres. O primeiro 2

dispositivo de comunicação exibe a cadeia de caracteres randômicos P selecionada e a primeira C1 cadeia de caracteres de verificação calculada no visor 7a (bloco 105) e, a cadeia de caracteres randômicos P e a cadeia C1 de caracteres de verificação são reportadas para o usuário do segundo 3 dispositivo de comunicação (seta 106). O usuário do segundo dispositivo de comunicação entra com a cadeia de caracteres (neste exemplo, 12 caracteres) apresentados pelo primeiro 2 dispositivo de comunicação com o dispositivo de entrada 8b para o segundo 3 dispositivo de comunicação (bloco 107). Logo após, o estágio de verificação é conduzido no segundo 3 dispositivo de comunicação. Assim, o segundo dispositivo de comunicação calcula a segunda C2 cadeia de caracteres de verificação (bloco 108) com base na cadeia de caracteres randômicos P e na chave de codificação compartilhada CH entrados pelo usuário. Depois disso, o segundo 3 dispositivo de comunicação compara a cadeia de caracteres C1 entrada pelo usuário com a segunda C2 cadeia de caracteres de verificação calculada (bloco 109). O segundo 3 dispositivo de comunicação indica o resultado da verificação, por exemplo, com um sinal e/ou no visor 7b, vantajosamente pelo menos quando as cadeias de caracteres de verificação C1, C2 não se associam (bloco 110). Assim, o usuário pode observar a situação e se abster de começar o processo de transmissão de dados. Se as cadeias de caracteres forem idênticas, pode ser assumido que a chave de codificação compartilhada CH é segura, isto é, com uma probabilidade forte de que a chave seja a mesma em ambos os dispositivos e esta pode ser usada na codificação de transmissão de dados e na conexão de transmissão de dados entre os dispositivos de comunicação 2, 3 que podem ser levados ao uso.

A informação a ser transmitida pela conexão de transmissão de dados estabelecida entre os dispositivos de comunicação 2, 3 é então codificada no dispositivo de comunicação transmissor com a chave de codificação compartilhada CH, onde a decodificação pode ser conduzida no dispositivo de comunicação receptor com a chave de codificação compartilhada CH correspondente.

Nos sistemas baseado na tecnologia Bluetooth™, a autenticação acima mencionada das partes tem de ser conduzidas apenas no estágio quando dois dispositivos de comunicação 2, 3 comunicam entre si pela primeira vez. Assim, o uso e a comparação de uma cadeia de caracteres de verificação relativamente curta de acordo com a invenção é

bastante fácil quando comparado às cadeias de caracteres da técnica anterior, por exemplo, o comprimento é tipicamente de pelo menos 32 caracteres. Em algumas incorporações práticas pode ser necessário conduzir as verificações mais de uma vez. Assim, uma segurança suficiente pode ser obtida com uma cadeia de caracteres de verificação curta, por exemplo, 8 caracteres podem ser um número suficiente de caracteres. Assim, o comprimento da cadeia de caracteres randômicos P é de 4 caracteres. Vantajosamente, o comprimento da cadeia de caracteres randômicos é de 4 a 8 números hexadecimais ou de 6 a 10 números decimais, onde as cadeias de caracteres de verificação correspondentes são de 8 a 18 números hexadecimais ou 12 a 20 números decimais longos.

No cálculo da primeira C1 cadeia de caracteres de verificação e da segunda C2 cadeia de caracteres de verificação a mesma função de cálculo é usada, que é, por exemplo, a função denominada hash. Tal função hash conduz a uma conversão para a entrada m e retorna uma cadeia de caracteres de comprimento fixo, que é denominada de valor hash h. Assim, matematicamente h = H(m). Nesta incorporação, a entrada que é usada é a chave de codificação compartilhada, que no primeiro dispositivo de comunicação é CH1 e que no segundo dispositivo de comunicação é CH2, e a cadeia de caracteres randômicos P. Assim, o primeiro dispositivo de comunicação executa a operação aritmética C1 = H(CH1,P) e o segundo dispositivo de comunicação executa a mesma operação aritmética C2 = H(CH2,P). Uma característica da função hash é que esta pode ser considerada como uma função de modo-único, isto é, com base no resultado calculado, este é, na prática, muito difícil, ou até mesmo impossível, determinar a entrada usada no cálculo. É óbvio que, em vez da função hash é também possível aplicar outro método, tal como o método de codificação de bloco.

A seguir, a operação do método de acordo com a segunda incorporação preferida da invenção será descrito com referência ao fluxo reduzido apresentado na Figura 2. Este método difere da incorporação preferida descrita acima nesta descrição principalmente no que diz respeito ao método de acordo com a segunda incorporação preferida, que utiliza os visores 7a, 7b de ambos os dispositivos de comunicação 2, 3 e os dispositivos de entrada 8b do segundo dispositivo de comunicação 3.

Na situação onde o objetivo é estabelecer uma conexão de transmissão de

dados entre o primeiro e o segundo dispositivos de comunicação, a seguir os passos são obtidos no método de acordo com a segunda incorporação preferida da invenção. Os dispositivos de transmissão de dados 2, 3 conduzem ao estágio de troca de chave (bloco 202) como apresentado anteriormente nesta descrição.

Nesta segunda incorporação preferida, o estágio de verificação é conduzido da maneira a seguir. O primeiro 2 dispositivo de comunicação seleciona uma cadeia de caracteres randômicos P relativamente curta (bloco 203) e visualiza a cadeia de caracteres randômicos P selecionada no visor 7a (bloco 204). A cadeia de caracteres randômicos P é reportada para o usuário do segundo 3 dispositivo de comunicação (seta 205). O usuário do segundo dispositivo de comunicação entra com a cadeia de caracteres randômicos P (neste exemplo, 6 caracteres) apresentada pelo primeiro 2 dispositivo de comunicação para o segundo 3 dispositivo de comunicação com o dispositivo de entrada 8b (bloco 206). Logo após, o segundo 3 dispositivo de comunicação calcula a segunda C2 cadeia de caracteres de verificação (bloco 208) com base na cadeia de caracteres randômicos P entrada pelo usuário e na chave secreta CH2, sendo esta apresentada no visor 7b (bloco 210). O primeiro 2 dispositivo de comunicação calcula a primeira C1 cadeia de caracteres de verificação (bloco 207) com base na cadeia de caracteres randômicos P entrada pelo usuário e na chave secreta CH1, sendo apresentada no visor 7a (bloco 209). Logo após, o usuário do primeiro 2 dispositivo de comunicação e o usuário do segundo 3 dispositivo de comunicação compara os cálculos dos dispositivos de comunicação e as cadeias de caracteres de verificação C1, C2 apresentadas pelo mesmo. Se as cadeias de caracteres de verificação C1, C2 correspondem entre si, o usuário do segundo 3 dispositivo de comunicação indica com o dispositivo de entrada 8 que as cadeias de caracteres se associam (bloco 211). Assim, a chave de codificação compartilhada CH é confiável, e esta pode ser usada na codificação da transmissão de dados e na conexão da transmissão de dados entre os dispositivos de comunicação 2, 3 que podem ser levados ao uso.

A Figura 3 apresenta o método de acordo com a terceira incorporação preferida da invenção. Também, nesta incorporação as chaves secretas CH1, CH2 são geradas nos dispositivos de comunicação 2, 3 usando algum protocolo de troca de chave conduzido entre os dispositivos de comunicação 2, 3 (bloco 302). Logo após, ambos os

dispositivos de comunicação 2, 3 indicam, vantajosamente, no visor 7a, 7b que o estágio de troca da chave tem sido conduzido (bloco 303) e os usuários dos dispositivos de comunicação 2, 3 informam entre si destes (bloco 304) (se os usuários em questão são diferentes). Neste estágio, o usuário do primeiro 2 dispositivo de comunicação, vantajosamente informa ao primeiro dispositivo de comunicação 2 com o dispositivo de entrada 8a que o estágio de troca da chave tem sido conduzido (bloco 305). Logo após, o primeiro 2 dispositivo de comunicação seleciona a primeira cadeia de caracteres randômicos P (bloco 306) e transmite esta por meio do dispositivo de comunicação local 4a para o segundo 3 dispositivo de comunicação (bloco 307). Em adição, o primeiro dispositivo de comunicação calcula o primeiro número de verificação, C1 (bloco 308), como foi descrito acima. O segundo 3 dispositivo de comunicação também calcula o segundo número de verificação C2 da maneira descrita acima (bloco 309). Após o cálculo, o primeiro 2 dispositivo de comunicação apresenta o primeiro número de verificação C1 e a cadeia de caracteres randômicos P no visor 7a (bloco 310). De maneira correspondente, o segundo 3 dispositivo de comunicação apresenta o segundo número de verificação C2 e a cadeia de caracteres randômicos P no visor 7b (bloco 311). Os usuários podem agora comparar os valores apresentados pelos dispositivos de comunicação 2, 3 e observar se a autenticação das partes tem sido conduzidas com sucesso (bloco 312). Se os valores apresentados se associam, o usuário do primeiro 2 dispositivo de comunicação indica com o dispositivo de entrada 8a que a conexão pode ser estabelecida (bloco 313). Como dispositivo de entrada 8a, por exemplo, uma chave é suficiente, mas é também possível usar um teclado, um dispositivo de controle de áudio, um dispositivo ponteiro ou um dispositivo correspondente como o dispositivo de entrada 8a.

No método de acordo com ainda outra incorporação preferida da invenção, ambos os dispositivos de comunicação 2, 3 executam um estágio de troca de chave interativo para gerar as mesmas chaves secretas Y1, Y2 em ambos os dispositivos. O estágio de troca da chave é conduzido usando, por exemplo, o protocolo de troca de chave Diffie-Hellman. Assim, no primeiro dispositivo de comunicação os parâmetros a, q são selecionados, o primeiro número secreto X1 é gerado, e o primeiro número de chave Y1 é calculado vantajosamente por meio da fórmula $Y1 = a^{X1} \bmod q$. O primeiro 2 dispositivo de

comunicação transmite os valores numéricos a, q, Y1 para o segundo 3 dispositivo de comunicação. O segundo 3 dispositivo de comunicação gera o segundo número secreto X2, calcula o segundo número da chave por meio da fórmula $Y2=a^{X2}$ mod q e transmite o segundo número de chave Y2 para o primeiro 2 dispositivo de comunicação. Após este estágio de troca de chave, o primeiro 2 dispositivo de comunicação calcula a primeira cadeia de caracteres de verificação C1 com base na cadeia de caracteres randômicos P gerado e no primeiro Y1 e no segundo número de chave Y2. O segundo 2 dispositivo de comunicação visualiza a cadeia de caracteres randômicos P selecionada e a primeira cadeia de caracteres de verificação C1 calculada no visor 7a e, a cadeia de caracteres randômicos P e a cadeia de caracteres de verificação C1 são reportadas para o usuário do segundo 3 dispositivo de comunicação. O usuário do segundo 3 dispositivo de comunicação entra com a cadeia de caracteres apresentada pelo primeiro 2 dispositivo de comunicação com o dispositivo de entrada 8b para o segundo 3 dispositivo de comunicação. Logo após, o estágio de verificação é conduzido no segundo 3 dispositivo de comunicação. Logo após, o estágio de verificação é conduzido no segundo 3 dispositivo de comunicação. Assim, o segundo dispositivo de comunicação calcula a segunda cadeia de verificação C2 com base na cadeia de caracteres randômicos P e no primeiro Y1 e no segundo número de chave Y2. Logo após, o segundo 3 dispositivo de comunicação compara a cadeia de caracteres C1 entrada pelo usuário com a segunda cadeia de caracteres de verificação C2 calculada. O segundo 3 dispositivo de comunicação indica o resultado da verificação, por exemplo, com o sinal e/ou no visor 7b, vantajosamente ao menos quando as cadeias de caracteres de verificação C1, C2 não se associam. Assim, o usuário pode observar a situação e refrear do inicio o processo de transmissão de dados. Se as cadeias de caracteres forem idênticas, pode ser assumido que o primeiro Y1 e o segundo Y2 número de chave são confiáveis, isto é, com uma forte probabilidade de que as chaves sejam as mesmas em ambos os dispositivos.

Em todas as incorporações preferidas apresentadas acima, o usuário do primeiro 2 dispositivo de comunicação e o usuário do segundo 3 dispositivo de comunicação podem ser pessoas diferentes, ou a mesma pessoa pode operar ambos os dispositivos de comunicação 2, 3. Se os usuários são duas pessoas diferentes, é possível reportar a soma de verificação C1, C2 oralmente ou por meio de outro método confiável, no

qual os usuários podem ter a certeza de que a informação tem sido realmente transmitida pela pessoa em questão, não por um estranho.

O método de acordo com a invenção pode ser aplicado especialmente em tais sistemas, nos quais a troca de chave é conduzida por meio do método baseado na codificação assimétrica, onde é possível prevenir a espionagem passiva, mas uma intervenção por uma terceira parte é possível. Em adição, deve ser possível verificar os dispositivos de comunicação 2, 3, isto é, tornando possível principalmente o uso nos sistemas de alcance limitado, nos quais os usuários podem ver ambos os dispositivos de comunicação 2, 3. Assim, a invenção é especialmente vantajosa nas conexões de transmissão de dados de alcance limitado, por exemplo no acoplamento sem fio dos dispositivos periféricos ao dispositivo de processamento de dados, quando o usuário está entrando na rede de área local sem fio por meio de um dispositivo de processamento de dados sem fio, etc.

É óbvio que a presente invenção não está limitada somente às incorporações apresentadas acima, mas pode ser modificada dentro do escopo das reivindicações apensas.

## REIVINDICAÇÕES

1. Método para assegurar uma transmissão de dados segura entre o primeiro (2) e o segundo (3) dispositivos de comunicação em uma comunicação sem fio de alcance-limitado na qual, para estabelecer uma conexão de transmissão de dados, os dispositivos (2, 3) de comunicação conduzem a um estágio de troca de chave para trocar ao menos duas chaves (Y1, Y2) entre os dispositivos (2, 3) de comunicação, e com base nas chaves trocadas (Y1, Y2) ao menos uma chave de codificação (CH1, CH2) é derivada nos dispositivos (2, 3) de comunicação, o método é **CARACTERIZADO** pelo fato de que no estágio de troca da chave ao menos a primeira (C1) e a segunda (C2) cadeia de caracteres de verificação são formadas, as cadeias de caracteres sendo baseadas nas chaves (CH1, CH2, Y1, Y2) derivadas ao menos no estágio da troca de chave, e onde a segurança da conexão estabelecida é assegurada ao comparar a correspondência das cadeias de caracteres de verificação (C1, C2).

2. Método de acordo com a reivindicação 1, é **CARACTERIZADO** pelo fato de que o primeiro dispositivo de comunicação determina a primeira (CH1) chave de codificação, o segundo dispositivo de comunicação determina a segunda (CH2) chave de codificação, a terceira chave de codificação (CH) é determinada para codificação da informação a ser transmitida na conexão de transmissão de dados, a cadeia de caracteres de verificação randômica (P) é também selecionada, o primeiro dispositivo de comunicação gera a primeira (C1) cadeia de caracteres de verificação com base ao menos na primeira (CH1) chave de codificação e na cadeia de caracteres randômicos (P), e o segundo dispositivo de comunicação gera a segunda (C2) cadeia de caracteres de verificação com base ao menos na segunda (CH2) chave de codificação e na cadeia de caracteres randômicos (P), e onde a primeira (C1) cadeia de caracteres de verificação e a segunda (C2) cadeia de caracteres de verificação são comparadas, onde, se as cadeias de caracteres de verificação corresponderem entre si, a terceira chave de codificação (CH) gerada no estágio de troca de chave é aceita para ser usada na conexão de transmissão de dados.

3. Método de acordo com a reivindicação 2, é **CARACTERIZADO** pelo fato de que para conduzir a comparação, o primeiro (2) dispositivo de comunicação apresenta ao menos a primeira (C1) cadeia de caracteres de verificação e ao menos a

primeira (C1) cadeia de caracteres é a entrada para o segundo (3) dispositivo de comunicação no qual a primeira (C1) e a segunda (C2) cadeia de caracteres são comparadas.

4. Método de acordo com a reivindicação 3, é **CARACTERIZADO** pelo fato de que a cadeia de caracteres randômicos (P) é selecionada no primeiro (2) dispositivo de comunicação e a cadeia de caracteres randômicos (P) é transmitida para o segundo (3) dispositivo de comunicação para formar a segunda (C2) cadeia de caracteres de verificação.

5. Método de acordo com a reivindicação 4, é **CARACTERIZADO** pelo fato de que para transmitir a cadeia de caracteres randômicos (P) para o segundo (3) dispositivo de comunicação, a cadeia de caracteres randômicos (P) é apresentada no primeiro (2) dispositivo de comunicação, onde a cadeia de caracteres randômicos (P) é entrada no segundo (3) dispositivo de comunicação.

6. Método de acordo com as reivindicações 3, 4 ou 5, é **CARACTERIZADO** pelo fato de que o segundo (3) dispositivo de comunicação indica o resultado da comparação ao menos na situação onde as cadeias de caracteres de verificação (C1, C2) não correspondem entre si.

7. Método de acordo com as reivindicações 3, 4, 5 ou 6, na qual o primeiro usuário usa o primeiro (2) dispositivo de comunicação e o segundo usuário usa o segundo (3) dispositivo de comunicação, o método é **CARACTERIZADO** pelo fato de que o primeiro usuário transmite a informação apresentada pelo primeiro (2) dispositivo de comunicação com um método não-eletrônico para o segundo usuário, onde o segundo usuário entra com a informação transmitida pelo primeiro usuário para o segundo (3) dispositivo de comunicação.

8. Método de acordo com as reivindicações 3, 4, 5 ou 6, na qual o usuário usa ambos o primeiro (2) dispositivo de comunicação e o segundo (3) dispositivo de comunicação, o método é **CARACTERIZADO** pelo fato de que o usuário entra com a informação apresentada pelo primeiro (2) dispositivo de comunicação para o segundo (3) dispositivo de comunicação.

9. Método de acordo com a reivindicação 1 ou 2, é **CARACTERIZADO** pelo fato de que para conduzir a comparação, o primeiro (2) dispositivo de comunicação apresenta ao menos a primeira (C1) cadeia de caracteres de verificação e o segundo (3)

dispositivo de comunicação apresenta ao menos a segunda cadeia de caracteres (C2) de verificação.

10. Método de acordo com a reivindicação 9, é **CARACTERIZADO** pelo fato de que o resultado da comparação é reportado para ao menos o primeiro (2) e o segundo (3) dispositivos de comunicação.

11. Método de acordo com a reivindicação 10, na qual o primeiro usuário usa o primeiro (2) dispositivo de comunicação e o segundo usuário usa o segundo (3) dispositivo de comunicação, o método é **CARACTERIZADO** pelo fato de que o usuário transmite a informação apresentada pelo primeiro (2) dispositivo de comunicação com o método não-eletrônico para o segundo usuário, onde o segundo usuário reporta o resultado da comparação para o segundo (3) dispositivo de comunicação.

12. Método de acordo com a reivindicação 10, na qual o primeiro usuário usa ambos o primeiro (2) dispositivo de comunicação e o segundo (3) dispositivo de comunicação, o método é **CARACTERIZADO** pelo fato de que o usuário reporta o resultado da comparação para o segundo (3) dispositivo de comunicação.

13. Método de acordo com as reivindicações 1 a 12, é **CARACTERIZADO** pelo fato de que as cadeias de caracteres de verificação (C1, C2) compreendem menos de 32 caracteres, vantajosamente de 4 a 20 caracteres, e preferivelmente de 4 a 10 caracteres.

14. Método de acordo com a reivindicação 2, é **CARACTERIZADO** pelo fato de que a cadeia de caracteres randômicos (P) compreende menos de 32 caracteres, vantajosamente de 4 a 20 caracteres, e preferivelmente de 4 a 10 caracteres.

15. Método de acordo com a reivindicação 14, é **CARACTERIZADO** pelo fato de que a cadeia de caracteres randômicos (P) é formada de números contidos em um sistema numérico conhecido como tal.

16. Método de acordo com a reivindicação 1, é **CARACTERIZADO** pelo fato de que ao menos a primeira (C1) e a segunda (C2) cadeia de caracteres de verificação são formadas baseadas nas chaves trocadas (Y1, Y2).

17. Sistema de comunicação (1) compreendendo ao menos o primeiro (2) e o segundo (3) dispositivos de comunicação, os dispositivos (4a, 4b) para estabelecer a conexão de transmissão de dados sem fio de alcance-limitado entre o primeiro (2) e o

segundo (3) dispositivos de comunicação, e um dispositivo para assegurar uma transmissão de dados segura na conexão de transmissão de dados, compreendendo um dispositivo para conduzir o estágio de troca de chave para trocar ao menos duas chaves (Y1, Y2) entre os dispositivos (2, 3) de comunicação, e um dispositivo para derivar ao menos uma chave de codificação com base nas chaves trocadas (Y1, Y2) nos dispositivos (2, 3) de comunicação, o método é **CARACTERIZADO** pelo fato de que o dispositivo para assegurar a transmissão de dados segura compreende um dispositivo para formar ao menos a primeira (C1) e a segunda (C2) cadeia de caracteres de verificação, as cadeias de caracteres sendo baseadas nas chaves trocadas (CH1, CH2, Y1, Y2) ao menos no estágio de troca da chave, e os dispositivos (4a, 4b, 7a, 7b) para comparar a correspondência das cadeias de caracteres de verificação (C1, C2).

18. Sistema de comunicação (1) de acordo com a reivindicação 17, é **CARACTERIZADO** pelo fato de que compreende um dispositivo para determinar a primeira (CH1) chave de codificação no primeiro (2) dispositivo de comunicação, um dispositivo para determinar a segunda (CH2) chave de codificação no segundo (3) dispositivo de comunicação, um dispositivo para determinar a chave de codificação de enlace (CH) para codificação da informação a ser transmitida na conexão de transmissão de dados, um dispositivo (5a, 5b) para selecionar a cadeia de caracteres de verificação randômica (P), um dispositivo (5a) para formar a primeira (C1) cadeia de caracteres de verificação no primeiro (2) dispositivo de comunicação, com base ao menos na primeira chave de codificação (CH1) e na cadeia de caracteres randômicos (P), e um dispositivo (5b) para formar a segunda (C2) cadeia de caracteres de verificação no segundo dispositivo (3) de comunicação, com base ao menos na segunda chave de codificação (CH2) e na cadeia de caracteres randômicos (P), e um dispositivo (7a, 7b) para comparar a primeira (C1) cadeia de caracteres de verificação e a segunda (C2) cadeia de caracteres de verificação, onde, se as cadeias de caracteres de verificação corresponderem entre si, a chave de codificação de enlace (CH) selecionada no estágio de troca de chave é disposta para ser usada na conexão de transmissão de dados.

19. Sistema de comunicação (1) de acordo com a reivindicação 18, é **CARACTERIZADO** pelo fato de que para conduzir a comparação, o primeiro (2)

dispositivo de comunicação compreende o dispositivo (7a) para apresentar ao menos a primeira (C1) cadeia de caracteres de verificação e, o segundo dispositivo (3) de comunicação compreende o dispositivo (8b) para entrar ao menos com a primeira (C1) cadeia de caracteres e, o dispositivo (5b) para comparar a primeira (C1) e a segunda (C2) cadeias de caracteres de verificação.

20. Sistema de comunicação (1) de acordo com a reivindicação 19, é **CARACTERIZADO** pelo fato de que a cadeia de caracteres randômicos (P) é selecionada no primeiro (2) dispositivo de comunicação e o sistema compreende os dispositivos (7a, 8b) para transmitir a cadeia de caracteres randômicos (P) para o segundo (3) dispositivo de comunicação para formar a segunda (C2) cadeia de caracteres de verificação.

21. Sistema de comunicação (1) de acordo com a reivindicação 19, é **CARACTERIZADO** pelo fato de que os dispositivos (7a, 8b) para transmitir a cadeia de caracteres de codificação para o segundo (3) dispositivo de comunicação compreendem o dispositivo (7a) para apresentar a cadeia de caracteres randômicos (P) no primeiro (2) dispositivo de comunicação, e o dispositivo (8b) para entrar com a cadeia de caracteres randômicos (P) apresentada no primeiro (2) dispositivo de comunicação para o segundo (3) dispositivo de comunicação.

22. Sistema de comunicação (1) de acordo com as reivindicações 19, 20 ou 21, é **CARACTERIZADO** pelo fato de que o segundo (3) dispositivo de comunicação compreende os dispositivos (7b, 10b) para reportar o resultado da comparação ao menos na situação onde as cadeias de caracteres de verificação (C1, C2) não correspondem entre si.

23. Sistema de comunicação (1) de acordo com a reivindicação 17, é **CARACTERIZADO** pelo fato de que o primeiro (2) dispositivo de comunicação compreende o dispositivo (7a) para apresentar ao menos a primeira (C1) cadeia de caracteres de verificação, e o segundo (3) dispositivo de comunicação compreende o dispositivo (7b) para apresentar ao menos a segunda (C2) cadeia de caracteres de verificação.

24. Sistema de comunicação (1) de acordo com a reivindicação 23, é **CARACTERIZADO** pelo fato de que ao menos o primeiro (2) e o segundo (3) dispositivos de comunicação compreendem os dispositivos (8a, 8b) para entrar com o resultado da

comparação.

25. Sistema de comunicação (1) de acordo com a reivindicação 17, é **CARACTERIZADO** pelo fato de que ao menos a primeira (C1) e a segunda (C2) cadeias de caracteres de verificação são formadas baseado nas chaves trocadas (Y1, Y2).

26. Dispositivo de comunicação (2, 3) compreendendo ao menos os dispositivos (4a, 4b) para estabelecer a conexão de transmissão de dados sem fio de alcance-limitado entre o dispositivo (3) de comunicação e os outros dispositivos (3, 2) de comunicação, e um dispositivo para assegurar uma transmissão de dados segura na conexão de transmissão de dados, compreendendo um dispositivo para conduzir o estágio de troca de chave com outro dispositivo de comunicação para trocar ao menos duas chaves (Y1, Y2) entre os dispositivos (2, 3) de comunicação, e um dispositivo para derivar ao menos uma chave de codificação com base nas chaves trocadas (Y1, Y2), o dispositivo é **CARACTERIZADO** pelo fato de que o dispositivo para assegurar a transmissão de dados segura compreende um dispositivo para formar ao menos uma cadeia de caracteres de verificação (C1, C2), a cadeia de caracteres sendo baseada ao menos nas chaves trocadas (CH1, CH2, Y1, Y2) no estágio de troca da chave e os dispositivos (4a, 4b, 7a, 7b) para comparar a correspondência das cadeias de caracteres de verificação (C1, C2).

27. Dispositivo de comunicação (2, 3) de acordo com a reivindicação 26, é **CARACTERIZADO** pelo fato de que compreende um dispositivo para determinar a chave de codificação (CH1), um dispositivo para determinar a chave de codificação de enlace (CH) para codificação da informação a ser transmitida na conexão de transmissão de dados, um dispositivo (5a, 5b) para selecionar a cadeia de caracteres de verificação randômica (P), um dispositivo (5a) para formar a primeira (C1) cadeia de caracteres de verificação ao menos com base na primeira (CH1) chave de codificação e na cadeia de caracteres randômicos (P), e um dispositivo (7a) para apresentar ao menos a cadeia de caracteres (C1) de verificação.

28. Dispositivo de comunicação (2, 3) de acordo com a reivindicação 26, é **CARACTERIZADO** pelo fato de que ao menos a primeira (C1) e a segunda (C2) cadeias de caracteres de verificação são formadas baseado nas chaves trocadas (Y1, Y2).

29. Dispositivo de comunicação (2, 3) de acordo com as reivindicações 26,

27 ou 28 é **CARACTERIZADO** pelo fato de que é um dispositivo de comunicação sem fio.

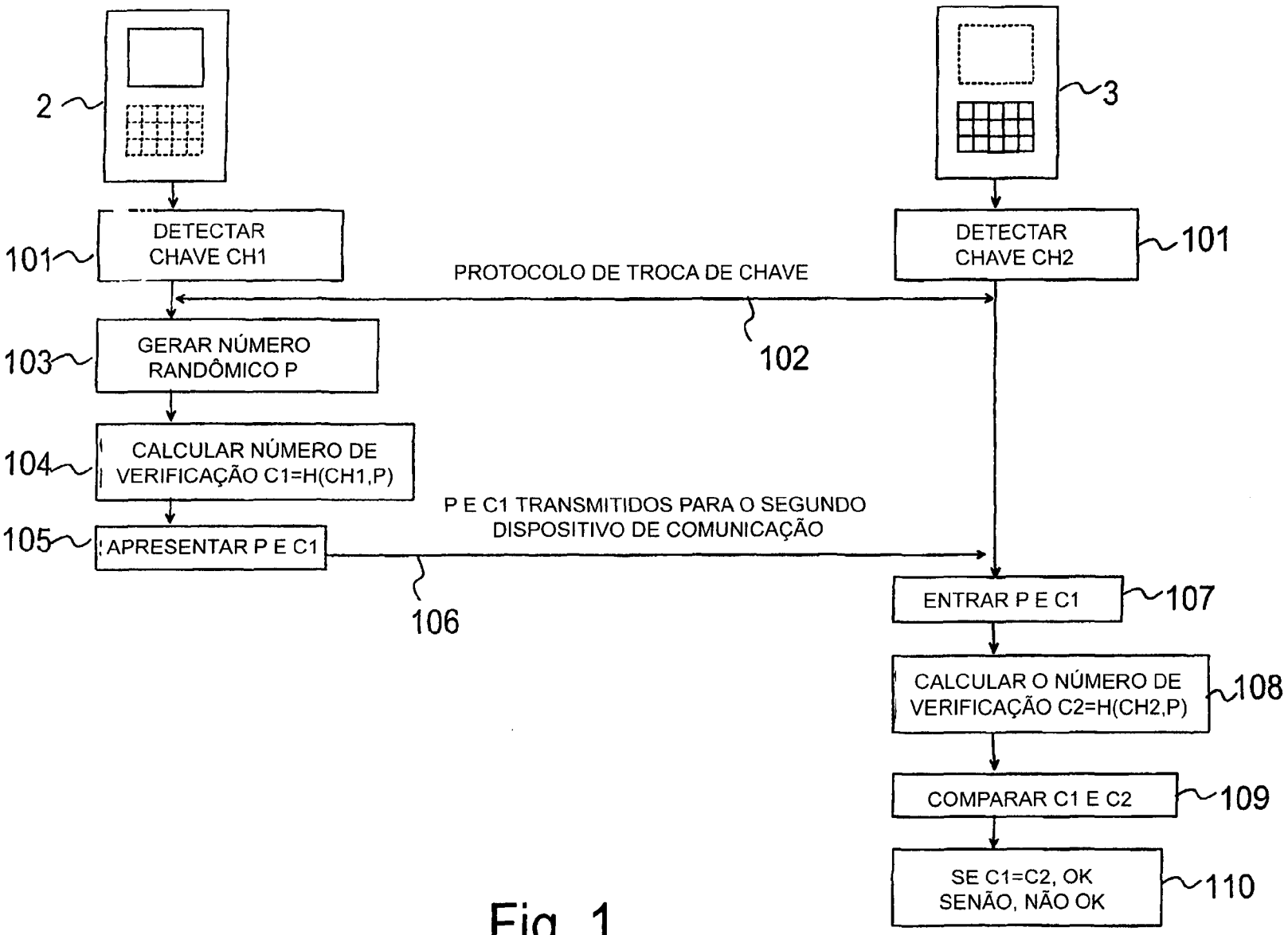
2
3
101
DETECTAR CHAVE CH1
DETECTAR CHAVE CH2
101
PROTOCOLO DE TROCA DE CHAVE
102
103
GERAR NÚMERO RANDÔMICO P
104
CALCULAR NÚMERO DE VERIFICAÇÃO C1=H(CH1,P)
105
APRESENTAR P E C1
P E C1 TRANSMITIDOS PARA O SEGUNDO DISPOSITIVO DE COMUNICAÇÃO
106
ENTRAR P E C1
107
CALCULAR O NÚMERO DE VERIFICAÇÃO C2=H(CH2,P)
108
COMPARAR C1 E C2
109
SE C1=C2, OK
SENÃO, NÃO OK
110

Fig. 1

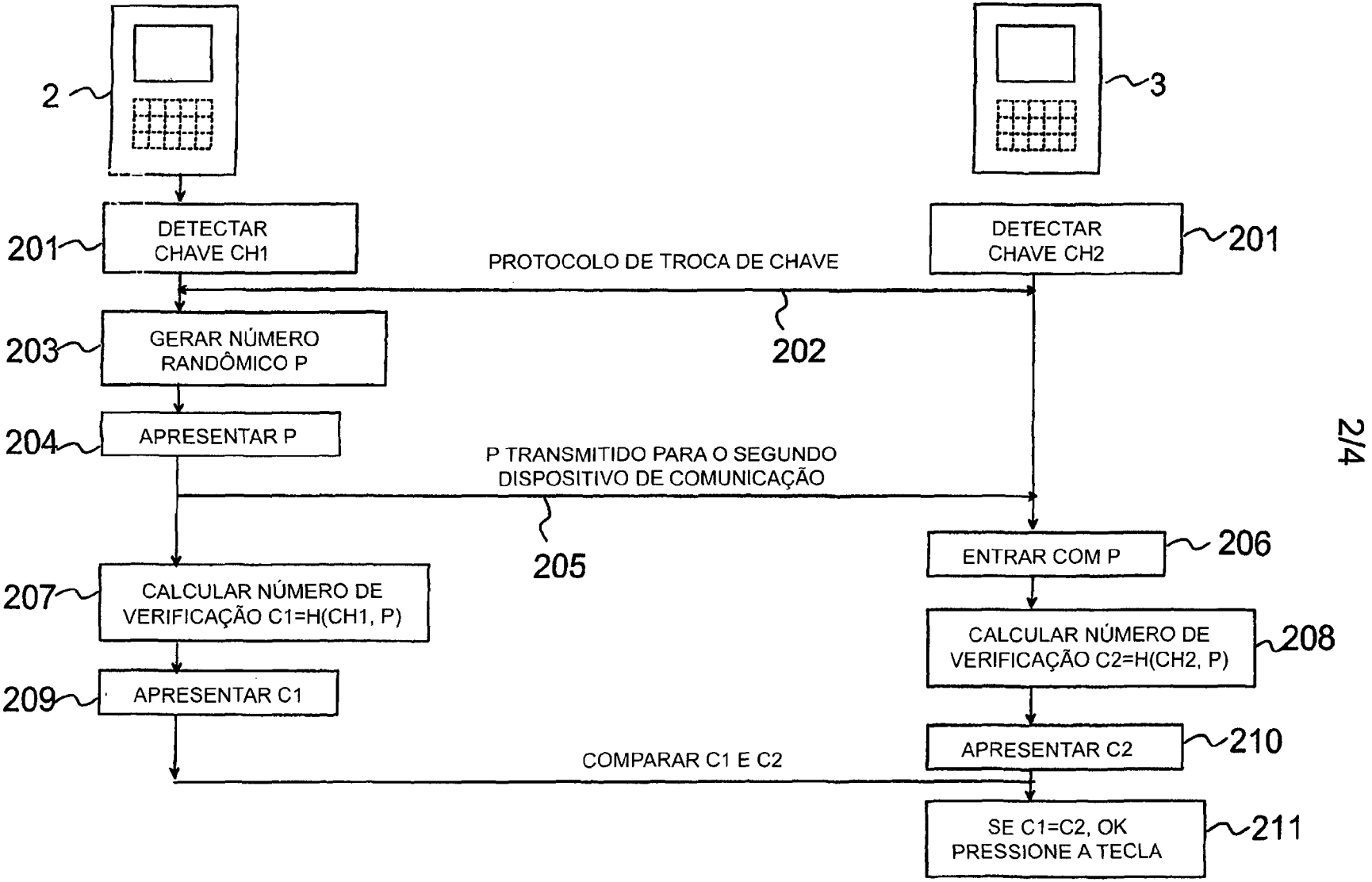
2
3
201
DETECTAR CHAVE CH1
DETECTAR CHAVE CH2
201
PROTOCOLO DE TROCA DE CHAVE
202
203
GERAR NÚMERO RANDÔMICO P
204
APRESENTAR P
P TRANSMITIDO PARA O SEGUNDO DISPOSITIVO DE COMUNICAÇÃO
205
ENTRAR COM P
206
207
CALCULAR NÚMERO DE VERIFICAÇÃO C1=H(CH1, P)
CALCULAR NÚMERO DE VERIFICAÇÃO C2=H(CH2, P)
208
209
APRESENTAR C1
APRESENTAR C2
210
COMPARAR C1 E C2
SE C1=C2, OK PRESSIONE A TECLA
211

Fig. 2

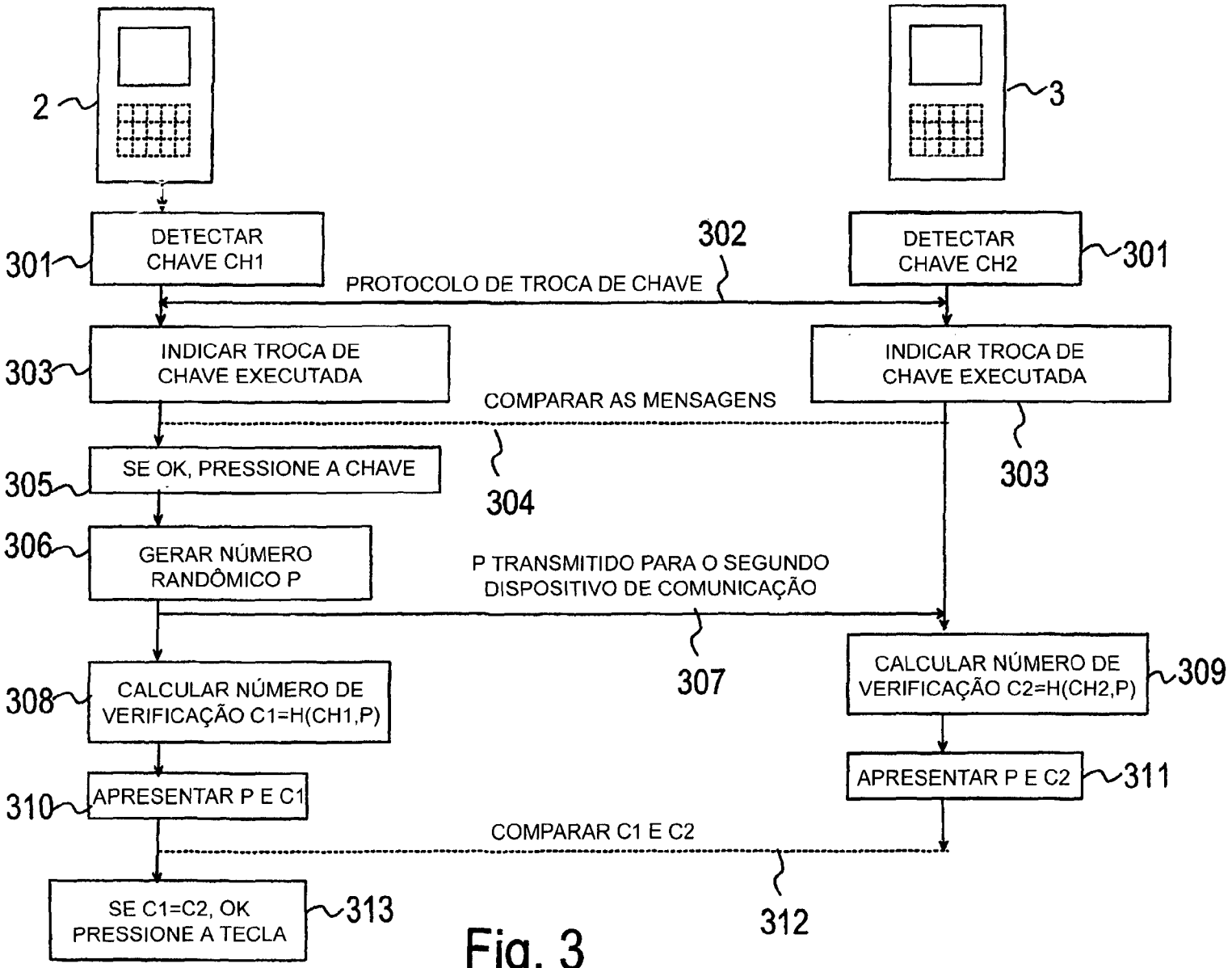
2
3
DETECTAR CHAVE CH1
301
302
DETECTAR CHAVE CH2
301
PROTOCOLO DE TROCA DE CHAVE
INDICAR TROCA DE CHAVE EXECUTADA
303
INDICAR TROCA DE CHAVE EXECUTADA
COMPARAR AS MENSAGENS
304
303
SE OK, PRESSIONE A CHAVE
305
GERAR NÚMERO RANDÔMICO P
306
P TRANSMITIDO PARA O SEGUNDO DISPOSITIVO DE COMUNICAÇÃO
307
CALCULAR NÚMERO DE VERIFICAÇÃO C1=H(CH1,P)
308
CALCULAR NÚMERO DE VERIFICAÇÃO C2=H(CH2,P)
309
APRESENTAR P E C1
310
APRESENTAR P E C2
311
COMPARAR C1 E C2
312
SE C1=C2, OK PRESSIONE A TECLA
313

Fig. 3

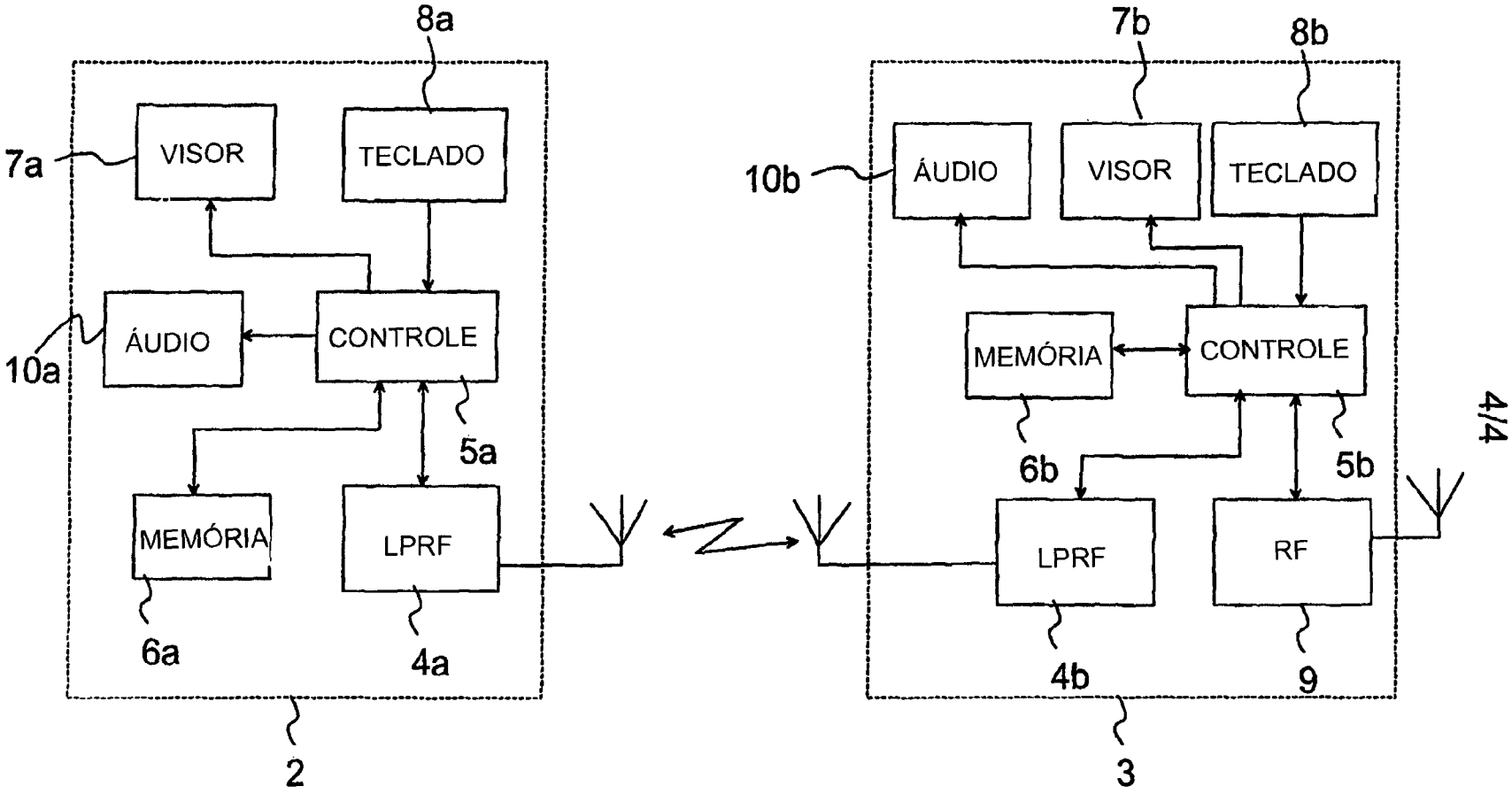
8a
7a
VISOR
TECLADO
10a
ÁUDIO
CONTROLE
5a
MEMÓRIA
LPRF
6a
4a
2
7b
8b
10b
ÁUDIO
VISOR
TECLADO
MEMÓRIA
CONTROLE
6b
5b
LPRF
RF
4b
9
3
4/4

Fig. 4

## RESUMO

**"MÉTODO E SISTEMA PARA ASSEGURAR UMA TRANSMISSÃO DE DADOS SEGURA ENTRE O PRIMEIRO E O SEGUNDO DISPOSITIVOS DE COMUNICAÇÃO EM UMA COMUNICAÇÃO SEM FIO DE ALCANCE LIMITADO, E, DISPOSITIVO DE COMUNICAÇÃO".**

A invenção descreve um método para assegurar uma transmissão de dados segura entre o primeiro (2) e o segundo dispositivo de comunicação (3) em uma comunicação sem fio de alcance-limitado. Para estabelecer uma conexão de transmissão de dados segura, os dispositivos de comunicação (2, 3) conduzem a um estágio de troca da chave para gerar ao menos uma chave compartilhada (CH) entre os dispositivos de comunicação. Após o estágio de troca da chave, ao menos a primeira (C1) e a segunda (C2) cadeias de caracteres de verificação são formadas, as cadeias de caracteres sendo baseadas ao menos em uma cadeia de caracteres randômicos única e nas chaves (CH1, CH2) geradas em cada dispositivo de comunicação no estágio de troca da chave. Assim, a segurança da conexão que é estabelecida é assegurada ao comparar a correspondência das cadeias de caracteres de verificação (C1, C2). A invenção também descreve um sistema de comunicação e um dispositivo de comunicação, no qual o método será aplicado.