República Federativa do Brasil

Ministério do Desenvolvimento, Indústria, Comércio e Serviços

Instituto Nacional da Propriedade Industrial

(21) BR 102024011043-9 A2

(22) Data do Depósito: 01/06/2024

(43) Data da Publicação Nacional: 09/12/2025

(54) Título: MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA

(51) Int. Cl.: H04L 9/06; H04L 9/14; H04L 9/08.

(52) CPC: H04L 9/06; H04L 9/14; H04L 9/08.

(71) Depositante(es): UNIVERSIDADE ESTADUAL PAULISTA JULIO DE MESQUITA FILHO.

(72) Inventor(es): CINTYA WINK DE OLIVEIRA BENEDITO; IVAN ARITZ ALDAYA GARDE; MARCELO LUÍS FRANCISCO ABBADE; THIAGO DE ANDRADE BRAGAGNOLLE; WELERSON SANTOS SOUZA; JOSÉ AUGUSTO DE OLIVEIRA; MIRIAN PAULA DOS SANTOS.

(57) Resumo: MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA. Trata a presente invenção de um novo método que atua no sentido de criptografar sinais discretos da chamada Subcamada Dependente do Meio na Camada Física de um sistema de comunicações, que é a camada responsável por converter a informação digital em sinais, o qual a partir de uma estratégia inédita em que as chaves criptográficas podem ser reutilizadas. O método proposto é referente à criptografia de sinais discretos. Esse método é o único conhecido que permite a reutilização da mesma chave criptográfica para encriptar blocos distintos. A reutilização da chave para encriptar diferentes blocos, que é amplamente utilizada em criptografia de dados, permite a encriptação paralela de vários blocos de sinais tornando o processo mais rápido e seguro, incorporando à criptografia de sinais e operações que são seguras e amplamente utilizadas na criptografia de dados.

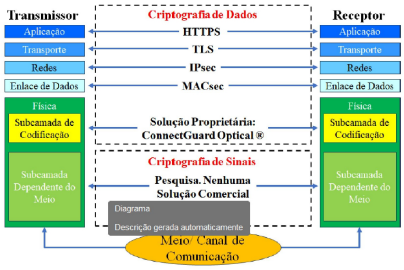

Figura 1

MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA

[001] Trata a presente invenção de um novo método que atua no sentido de criptografar sinais discretos da chamada Subcamada Dependente do Meio na Camada Física de um sistema de comunicações, que é a camada responsável por converter a informação digital em sinais, o qual a partir de uma estratégia inédita em que as chaves criptográficas podem ser reutilizadas. O método proposto é referente à criptografia de sinais discretos. Esse método é o único conhecido que permite a reutilização da mesma chave criptográfica para encriptar blocos distintos. A reutilização da chave para encriptar diferentes blocos, que é amplamente utilizada em criptografia de dados, permite a encriptação paralela de vários blocos de sinais tornando o processo mais rápido e seguro, incorporando à criptografia de sinais e operações que são seguras e amplamente utilizadas na criptografia de dados.

CAMPO DA INVENÇÃO

[002] O método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, é aplicado nos sistemas de comunicação na criptografia de sinais, sistemas que operam com uma divisão hierárquica de camadas onde cada camada desempenha um conjunto de funções bem definido e oferece serviços à camada imediatamente superior da arquitetura utilizada.

[003] O método aqui proposto encripta sinais discretos em banda-base. Os sinais encriptados podem então ser modulados em portadoras de qualquer frequência, propagados até o receptor, demodulados e desencriptados. Assim, o método pode ser aplicado a sinais em qualquer enlace de comunicação digital ou analógico. São exemplos desses enlaces: enlaces de sinais em banda-base (como em redes Ethernet), enlaces de TV digital, enlaces de sinais sem fio (como em redes celulares) e enlaces de sinais ópticos. O método também pode ser utilizado para encriptar sinais que trafeguem por redes transparentes. Aqui, entende-se que uma rede é um

conjunto de enlaces interligados por nós de processamento. Entende-se que uma rede transparente é aquela em que os nós de processamento não precisam interpretar o conteúdo dos dados recebidos. São exemplos de redes transparentes, as redes ópticas transparentes, as redes ópticas passivas e redes de comunicação sem fio em que o nó de processamento é um satélite que simplesmente recebe um sinal em uma dada frequência, demodula esse sinal e o modula em uma nova frequência. Sendo assim, são exemplos de tecnologias que podem utilizar o método proposto: linha digital de assinante, 4G, 5G, Internet das Coisas, Fiber-to-the-Home, Fiber-to-the-Building, entre outras.

OBJETIVO DA INVENÇÃO

[004] O método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, tem por objetivo principal oferecer ao campo pertinente um método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, de forma segura e paralelizável, com a criptografia realizada a partir de uma estratégia inédita em que as chaves criptográficas podem ser reutilizadas.

FUNDAMENTOS

[005] As mensagens de um sistema de comunicações são constituídas por um conjunto de bits. Nas cifras de bloco esses bits são agrupados em unidades chamadas de blocos, que podem ser encriptados por diferentes técnicas e padrões comerciais, usados para prover confidencialidade à comunicação. Exemplos desses padrões são o Advanced Encryption Standard (AES) e o Tiny Encryption Algorithm (TEA). A encriptação é feita por um transmissor autorizado que utiliza um algoritmo e uma chave de encriptação. Vários blocos podem ser encriptados pela mesma chave. O algoritmo e a chave de encriptação são conhecidos pelos receptores autorizados e são usados para descriptografar os blocos de bits que constituem as mensagens. A Camada Física de um sistema de comunicação converte os bits das mensagens para sinais que trafegam por enlaces e demais elementos do sistema de comunicação. A informação de um ou mais bits é impressa nesses sinais a partir do

controle de grandezas físicas, como fases, amplitudes e frequências, de campos eletromagnéticos ou de correntes e tensões elétricas. Esses sinais são propagados até o receptor por meio de um enlace ou uma rede de comunicação. Tipicamente, esses sinais não são criptografados e isso gera uma brecha na segurança do sistema de comunicação. Propostas apresentadas na literatura sugerem que esses sinais podem ser criptografados desde que uma chave distinta seja calculada para encriptar o sinal referente a cada bloco. Dessa maneira, uma primeira chave é usada para encriptar um primeiro bloco. Uma segunda chave é calculada a partir da primeira chave e usada para encriptar o segundo bloco e assim sucessivamente.

[006] As perdas anuais por cybercrimes são da ordem US$ 600 bilhões de dólares por ano (cerca de 0,6% do PIB mundial). Isso estimula um investimento anual de cerca de US$ 100 bilhões por ano na área de segurança de rede. Grande parte dos problemas de segurança de rede pode ser resolvido com o uso de criptografia.

[007] Atualmente existem vários esquemas para criptografar os dados armazenados em computadores. No entanto, a transmissão de informação por redes (ou enlaces) de comunicação requer a conversão desses dados (conjunto de bits) em sinais elétricos ou eletromagnéticos. Esses sinais são propagados entre o transmissor e o receptor por uma infraestrutura (rede, enlaces) que, normalmente, não pertence aos proprietários legítimos da informação (transmissor e receptor). Em geral, essa infraestrutura é susceptível a ações de espiões e não pode ser monitorada pelas partes legitimamente envolvidas na comunicação. Se a propagação do sinal ocorrer pelo ar, é virtualmente impossível detectar a ação de espiões em sistemas atuais. Mesmo quando a comunicação ocorre por meios confinados, como fibras ópticas, os espiões podem usar equipamentos não-intrusivos (como os "optical clip-on couplers", aqui traduzido por "grampos ópticos") para ter acesso não autorizado à informação do transmissor e do receptor. A identificação desse tipo de espionagem é possível, mas nem sempre ocorre porque a monitoração das redes ópticas é complexa e porque as perdas introduzidas pelos equipamentos de espionagem são baixas e podem ser confundidas com as perdas por propagação nas fibras ou de inserção em

dispositivos/ equipamentos ópticos. De fato, a literatura aponta vários relatos de espionagem em cabos ópticos.

[008] Evidencia-se, portanto, que há uma falha de segurança durante a propagação de sinais por enlaces e/ou redes de telecomunicações. A solução para esse problema é criptografar os sinais transmitidos. Não se conhece nenhuma solução comercialmente disponível para realizar tal criptografia.

PROBLEMA A SER RESOLVIDO

[009] A criptografia é um recurso extensamente utilizado para prover confidencialidade e integridade à informação em sistemas de comunicação. Os sistemas de comunicação operam com uma divisão hierárquica de camadas, em que cada camada desempenha um conjunto de funções bem definido e oferece serviços à camada imediatamente superior da arquitetura utilizada. Existem soluções comerciais de criptografia para todas as camadas de comunicação, exceto para a subcamada inferior da Camada Física, chamada de Subcamada Dependente do Meio. Esta subcamada é responsável por converter a informação digital em sinais. A ausência de criptografia nesta subcamada é crítica porque cria uma falha de segurança referente aos sinais que se propagam do transmissor ao receptor autorizados por meio de enlaces e de redes que, normalmente, não pertencem às partes legítimas da comunicação (o transmissor e o receptor autorizados). Sendo assim, criptografar estes sinais é de suma importância para aumentar a segurança dos sistemas de comunicações atuais.

[010] Assim, o método aqui proposto atua no sentido de criptografar sinais da chamada de Subcamada Dependente do Meio, que é a responsável por converter a informação digital em sinais, a partir de uma estratégia inédita em que as chaves criptográficas podem ser reutilizadas. Infelizmente, a literatura atual não faz uma distinção clara entre os tipos de criptografia que podem ser utilizados na Camada Física. Além disso, a abordagem utilizada para realizar a criptografia de sinais é distinta daquela usada para criptografar dados nas camadas superiores.

[011] O método proposto é referente à criptografia de sinais discretos. Esse método é o único conhecido que permite a reutilização da mesma chave criptográfica para encriptar blocos distintos. A reutilização da chave para encriptar diferentes blocos, que é amplamente utilizada em criptografia de dados, permite a encriptação paralela de vários blocos de sinais tornando o processo mais rápido.

[012] Além disso, o método proposto pode incorporar à criptografia de sinais operações que são seguras e amplamente utilizadas na criptografia de dados. No melhor de nosso conhecimento, nenhum outro método de criptografia de sinais discretos permite tal equivalência, que pode estimular a utilização comercial do método por clientes que já estão habituados e que confiam nos procedimentos usados na criptografia de dados.

ESTADO DA TÉCNICA

[013] Os sistemas de comunicação são usualmente organizados em uma estrutura hierárquica de camadas. Cada camada desempenha um conjunto bem definido de funções, por meio de protocolos de comunicação, e oferece serviços à camada que lhe é imediatamente superior. A Figura 1 ilustra uma possível arquitetura com cinco camadas de comunicação. A camada inferior é a Camada Física, cujas funções são divididas entre duas subcamadas. A subcamada superior é chamada de Subcamada de Codificação e opera, por exemplo, para agregar bits em símbolos. Assim como as camadas superiores à Camada Física, a Subcamada de Codificação também lida com informações digitais. A subcamada inferior da Camada Física converte a informação digital para sinais. Esse processo, normalmente, é realizado por meio da conversão de palavras digitais para amostras dos sinais. Cada amostra é totalmente caracterizada por uma amplitude e por uma fase. Amplitudes e fases são, inerentemente, grandezas analógicas.

[014] Na visão atual, a segurança de um sistema de comunicações é maior quando cada camada/ subcamada implementa seu próprio esquema de encriptação. Há soluções comerciais de encriptação para todas as camadas superiores à Camada Física e para a subcamada de Codificação.

[015] Como todas essas criptografias lidam com informação digital, as técnicas de criptografia usadas nelas são chamadas de “criptografia de dados”. Os princípios da criptografia de dados foram em grande parte estabelecidos por Shannon em seu artigo seminal de 1949. Conforme ilustrado na Fig. 1, exemplos de protocolos comerciais de criptografia de dados são o HyperText Transfer Protocol Secure (HTTPs) para a Camada de Aplicação, o Transport Layer Security (TLS) para a Camada de Transporte, o Internet Protocol Security (IPSec) e o Media Access Control Security (MACSec) para a Camada de Enlace de Dados. A Subcamada de Codificação conta com soluções comerciais proprietárias como o ConnectGuard Optical® da empresa ADVA. Não há, no entanto, no melhor de nosso conhecimento, soluções comerciais para encriptação na Subcamda Dependente do Meio. Como essa subcamada lida com sinais, chamaremos seu processo de encriptação de “criptografia de sinais”. O método aqui proposto refere-se a uma proposta de criptografia de sinais. Diferente da criptografia de dados, que lida com informação digital, a criptografia de sinais discretos opera sobre amplitudes e fases, que são grandezas analógicas.

[016] Existem alguns documentos como artigos e documentos de patente que descrevem métodos de criptografia utilizando diferentes técnicas e algoritmos, contudo nenhum desses documentos antecipa a técnica apresentada no método aqui proposto. Dentre esses documentos pode-se destacar o seguinte:

[017] O documento de patente WO2015097312A1, *A HARMONIC BASED ENCRYPTION AND DECRYPTION SYSTEM FOR WAVEFORM SIGNALS*, o qual descreve um método para proteger um sinal de forma de onda para transmissão, convertendo o sinal no domínio da frequência, aplicando uma função de criptografia ao sinal convertido e, em seguida, aplicando uma conversão inversa para gerar o sinal criptografado final. A função de criptografia é uma cifra de Vernon, ou seja, correspondente a um bloco único. O processo é revertido para descriptografia. São apresentadas técnicas de supressão de ruído, sincronização e paralelização de hardware.

[018] Esse documento pode ser considerado de Baixa Relevância: essa invenção revela técnicas para fornecer uma cifra de sinal de camada física eficiente e segura, capaz de criptografar qualquer sequência de valores potencialmente ilimitada. Em particular, pode ser usado para criptografar sinais de comunicação como sinais de forma de onda (representando um sinal analógico) independentemente do conteúdo do canal (quadros, bits, modulações analógicas como FM ou AM, e até mesmo modulações binárias como QAM, FSK e assim por diante). Pode ser usado também para preservar a largura de banda do sinal original após a criptografia e para fornecer proteção absoluta aos canais subjacentes que abrangem alguma banda de frequência.

DESCRIÇÃO DAS FIGURAS

[019] A seguir faz-se referência às Figuras que acompanham este relatório descritivo, para melhor entendimento e ilustração do mesmo, onde se vê:

[020] A Figura 1 mostra um esquema a Arquitetura de Redes com 5 Camadas Hierárquicas com exemplos de soluções de criptografia de dados, do estado da técnica.

[021] A Figura 2 mostra um esquema da troca de chaves iniciais e operação das chaves de bloco, que conduzem a um processo serial de encriptação. As linhas vermelhas indicam a necessidade de cálculos para obter as chaves de bloco do bloco seguinte. Esses cálculos podem depender apenas de parâmetros das chaves de bloco imediatamente anteriores ou, dependendo da estratégia, de mais chaves anteriores também.

[022] A Figura 3 mostra Diagramas de bloco ilustrando que (a) um sistema de encriptação de sinais discretos N-dimensional pode ser reduzido a (b) um sistema de encriptação bidimensional que codifica a amplitude e a fase das amostras.

[023] A Figura 4 mostra Diagrama de blocos para a proposta de encriptação de sinais do método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção.

[024] A Figura 5 mostra o Diagrama de blocos para a proposta de desencriptação de sinais do método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção.

[025] A Figura 6 mostra os Diagramas de blocos para os (a) AES e (b) s-AES.

[026] A Figura 7 mostra os Diagramas de blocos para o s-AES operando no modo s-CTR.

[027] A Figura 8 mostra um diagrama de blocos do exemplo considerado para a técnica do método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, onde: (a) Exemplo de aplicação da técnica proposta com os algoritmos de encriptação s-AES e s-Permut. Operações internas (b) do s-AES e (c) dos blocos de Processamento.

[028] A Figura 9 mostra Espectros de sinais 16-QAM* de 28 Gbaud. (a) Espectro de amplitude para a média de 500 sinais NE, (b) Espectro de fase para a média de 500 sinais NE, (c) Espectro de fase para um sinal NE, (d) Espectro de amplitude para a média de 500 sinais E, (e) Espectro de fase para a média de 500 sinais E, (f) Espectro de fase para um sinal E, (g) Espectro de amplitude para a média de 500 sinais ED, (h) Espectro de fase para a média de 500 sinais ED, (i) Espectro de fase para um sinal ED.

[029] A Figura 10 mostra as Constelações dos sinais 16-QAM* (a) NE, (b) E e (c) ED.

[030] A Figura 11 mostra os Histogramas de amplitudes dos sinais 16-QAM* (a) NE, (b) E e (c) ED.

[031] A Figura 12 mostra os Histogramas de fases dos sinais 16-QAM* (a) NE, (b) E e (c) ED.

[032] A Figura 13 mostra as Curvas de sensibilidade para os sinais NE, E e DE em um canal AWGN.

[033] A Figura 14 mostra os Desempenho da propagação de sinais ED por um conjunto de enlaces ópticos.

[034] A Figura 15 mostra o Histograma da diferença de bits dos textos cifrados causada pela variação de um bit na mensagem. Resultados válidos para o s-AES, utilizando um sinal 16-QAM, e para o AES.

[035] A Figura 16 mostra a Correlação entre os bits distintos de textos cifrados obtidos a partir da encriptação de uma mesma mensagem com uma mesma chave criptográfica pelo s-AES e pelo s-CTR.

[036] A Figura 17 mostra a Relação entre a BER e o máximo desvio de fase, $\Delta\theta$, que pode ser tolerado pelo interceptador. Admite-se que as amplitudes de todas as amostras são conhecidas pelo interceptador.

[037] A Figura 18 mostra a Relação entre a BER e o número de amostras cujas amplitudes e fases são conhecidas pelo interceptador. Admite-se que as fases das demais amostras são também conhecidas.

[038] A Figura 19 mostra a Dependência entre o número de ataques e o número de amostras que deve ser conhecido pelo interceptador para recuperar o sinal no limite da FEC. Os números indicados em alguns pontos das curvas correspondem aos valores de $\Delta\theta$ expressos em graus.

DESCRIÇÃO GERAL DA INVENÇÃO

[039] O método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, é relacionado à criptografia de sinais discretos. Sinais são gerados e processados na Camada Física dos sistemas de comunicação e, muitas vezes, a literatura da área não faz uma divisão clara entre criptografia de sinais discretos e outros tipos de criptografia realizados na Camada Física.

[040] A Camada Física é dividida na Subcamada de Codificação e na Subcamada Dependente do Meio. A primeira destas subcamadas realiza operações como a conversão de bits em símbolos e opera com unidades de informação digitais (bits símbolos, grupos de símbolos). Já existem soluções comerciais de encriptação para esta subcamada. Na subcamada dependente do meio a informação digital é convertida para sinais físicos. Assim, as unidades de informação desta subcamada

correspondem às propriedades físicas destes sinais, como amplitude, fase e frequência. A criptografia aplicada nessa subcamada é frequentemente referida como "criptografia de sinais" e não dispõem de soluções comerciais, até o presente método.

[041] A seguir descrevem-se os tipos de Criptografia de Sinais

[042] A criptografia de sinais pode ser baseada na mecânica quântica, situação em que é chamada de criptografia quântica, ou em física clássica.

A. Criptografia Quântica de Sinais

[043] A criptografia quântica de sinais é baseada em fenômenos quânticos fundamentais, como o teorema da não-clonagem, associados a protocolos, como BB84 e o E91. Essas estratégias permitem identificar quando o sistema de comunicação está sob a ação de espionagem. Apesar da utilidade de tal característica, os fenômenos quânticos fundamentais estão sujeitos a um limite taxa-distância, descrito na literatura.. Para sistemas sem repetidores quânticos, observa-se, por exemplo que para um enlace de 100 km de comprimento, a máxima taxa de transmissão é de ~10 Mbits/s. Se o comprimento do enlace for aumentado para, por exemplo, 200 km, essa taxa é reduzida para ~200 kbits/s. Tais valores indicam que a criptografia quântica de sinais não pode ser usada para encriptar sinais de redes ópticas de sinais que, atualmente, operam a centenas de Gbits/s com sinais propagados por várias centenas de quilômetros. Por essas razões, a criptografia quântica de sinais é restrita a aplicações que requerem baixa taxa de transmissão, como a distribuição de chaves criptográficas quânticas (quantum key distribution, QKD).

[044] A invenção aqui proposta aplica-se à criptografa de sinais de qualquer taxa de transmissão propagados por qualquer distância. Dada a discussão anterior, as técnicas de criptografia quântica estão fora do escopo e não constituem um elemento concorrente à invenção aqui comunicada. Na verdade, o método aqui proposto pode atuar em conjunto com a QKD. Nessa estratégia, a QKD alimentaria o transmissor e o receptor com chaves criptográficas que comprovadamente não foram sujeitas à

espionagem e essas chaves seriam então usadas em nossos algoritmos de criptografia para encriptar sinais a altas taxas de transmissão.

B. Criptografia de Sinais baseada em Física Clássica

[045] A criptografia de sinais, fundamentada em uma abordagem de Física clássica, é a única que se alinha às taxas de transmissão presentes em todos os sistemas de comunicação modernos. Sinais podem estar em banda-base ou podem ser modulados. Assim, a criptografia de sinais baseada em Física Clássica pode ser realizada sobre essas duas classes que serão abordadas a seguir.

[046] A criptografia clássica de sinais modulados é considerada na literatura, sobretudo, sobre sinais modulados em portadoras ópticas. Apesar do interesse acadêmico no assunto, a criptografia de sinais modulados requer equipamentos específicos que encarecem o custo do sistema de comunicação. Além disso, estes equipamentos demandam operações no receptor que precisam desfazer exatamente o processo de encriptação realizado no transmissor. Este processamento pode não ser trivial. Por exemplo, há dificuldades para o receptor sincronizar-se com a portadora na técnica de criptografia caótica analógica. Já no caso da criptografia por fatiamento espectral, um ligeiro desalinhamento entre as fatias geradas no receptor e no transmissor pode degradar a qualidade do sinal desencriptado.

[047] Existem diversas técnicas disponíveis para a criptografia de sinais em banda-base. A grande vantagem desta abordagem é a possibilidade de utilização de processadores digitais de sinais (digital signal processors, DSPs), que são conhecidos por sua flexibilidade de programação. Além disso, como muitos sistemas de comunicação atuais já utilizam estes processadores, o custo para acrescentar algoritmos de criptografia de sinais a estes sistemas é bastante reduzido. Observa-se que a utilização de DSPs pressupõe a discretização de sinais. Por isso, nesta invenção esses sinais são denominados como “sinais discretos” e à criptografia associada a estes sinais como “criptografia de sinais discretos”.

[048] A literatura da área aponta várias técnicas para criptografar sinais, entre as quais: embaralhamento de amostras no domínio do tempo, embaralhamento de

amostras no domínio da frequência, codificação espectral de fase no domínio do tempo, codificação espectral de fase no domínio da frequência, codificação de amplitude no domínio do tempo, codificação espectral de amplitude, adição de ruído artificial, mapeamento de raio e desvio de fase, entre outras. Todas essas técnicas podem ser aplicadas a sinais de portadora única ou de múltiplas portadoras. No entanto, sinais de portadora múltipla também podem se valer de técnicas como codificação de fase de filtro e codificação de fase de sub-portadora.

[049] Em princípio, essas técnicas podem ser combinadas entre si de maneiras variadas. No entanto, mostrou-se recentemente que é suficiente codificar a fase e a amplitude de sinais discretos para obter a maior segurança possível. Além disso, também se pode notar que o embaralhamento de amostras é uma maneira equivalente e rápida de codificar a amplitude de sinais discretos. Assim, os sistemas seguros de criptografia de sinais discretos podem conter apenas dois estágios, sendo que um codifica a fase e outro embaralha as amostras. Apesar de essas operações poderem ser realizadas no domínio do tempo ou no domínio da frequência, a implantação no segundo desses domínios tem a vantagem de fazer com que a banda do sinal encriptado seja a mesma do sinal não encriptado.

[050] Os trabalhos da literatura sobre criptografia de sinais discretos consideram que o transmissor e o receptor secretamente trocam uma ou mais chaves criptográficas, aqui chamadas de “chaves iniciais”. A partir das chaves iniciais, em muitos casos, são calculadas novas chaves e cada nova chave é usada para encriptar apenas um único bloco de informação. A primeira chave encripta o primeiro bloco, a segunda chave encripta o segundo bloco e assim sucessivamente. As chaves que encriptam um único bloco são denominadas de “chaves de bloco”. A Figura 2 ilustra a atuação de chaves de blocos, evidenciando que esse esquema implica em uma estratégia de encriptação serial.

[051] Após um certo número de blocos enviados ao transmissor, que facilmente pode exceder a casa de milhares, há uma nova troca de chaves iniciais entre o transmissor e o receptor e o processo anterior é repetido. A utilização de chaves de bloco oferece

mecanismos de segurança como difusão, confusão e aleatoriedade de encriptação à informação, quando os sinais são convertidos para o domínio digital.

[052] Dentre as estratégias comumente usadas para gerar as chaves de bloco, destacam-se a criptografia caótica digital e as cifras de fluxo.

[053] Na primeira destas estratégias, as chaves obtidas para cifrar uma mensagem são obtidas a partir da solução de um sistema caótico alimentado com parâmetros usados para criar a chave que cifrou a mensagem anterior. No entanto, sistemas caóticos são determinísticos e, por esta razão, sua aplicação a soluções criptográficas recebe críticas na literatura. De fato, estes sistemas não são usados em soluções comerciais de criptografia. Cifras de fluxo são utilizadas em criptografia de dados, mas provêm difusão limitada e são vulneráveis a ataques de "bit flipping".

[054] Outra alternativa é produzir as chaves por meio de geradores pseudoaleatórios. Esses geradores, normalmente, usam funções de mão única para gerar chaves pseudoaleatórias. Essa abordagem pode ser usada em uma estratégia serial, como as descritas anteriormente, em que uma chave depende da anterior. Uma outra estratégia é utilizar o gerador pseudoaleatório em um modo de operação paralelizável, como o CTR. Alguns trabalhos da literatura fazem menção a essa possibilidade, mas não apresentam os detalhes de sua implementação.

[055] Nas codificações de amplitude e de fase para a criptografia de sinais, utilizando as técnicas de Codificação de Amplitude-Fase como Blocos Fundamentais da Criptografia de Sinais, um esquema linear N-dimensional pode ser substituído por um bidimensional que depende exclusivamente de uma combinação de codificação de amplitude (amplitude enocding, AE) e de codificação de fase (phase encoding, PE). Essa equivalência é uma consequência direta das amostras serem totalmente descritas por suas amplitudes e fases (Figura 3).

DESCRIÇÃO DETALHADA DA INVENÇÃO

[056] O método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, é relacionado à criptografia de sinais discretos.

[057] Como realização exemplar a seguir descreve-se o procedimento do método que encripta a informação de um vetor de inicialização que contém um contador. Sendo equivalente à operação do *Counter Mode* (CTR) em criptografia de dados.

[058] Conforme mostrado na Figura 4(a) que mostra um diagrama de blocos do método da presente invenção. Um vetor de inicialização IV_1, também identificado por β_1, é composto por um *nonce* e por um contador. Para IV_1 o contador está, por exemplo, ajustado em zero. A Subcamada de Codificação (SC) mapeia IV_1 em símbolos de sinais. Esses símbolos podem ser, por exemplo, referentes ao equivalente complexo em banda-base de um sinal com modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM) de ordem M arbitrária (M-QAM). Opcionalmente, esses símbolos podem ser processados pelo bloco Processamento1, na própria SC ou na Subcamada Dependente do Meio (SDM). Um exemplo de processamento na SC é o embaralhamento de símbolos. Um exemplo de processamento na SDM é a limitação de banda do sinal por meio de filtragem. As operações na SDM podem ocorrer no domínio do tempo, no domínio da frequência ou em ambos.

[059] A seguir, o sinal processado é submetido ao Algoritmo de Encriptação de Sinal1, E_1, que também é alimentado com a Chave1, k_1.

[060] No digrama de blocos da Figura 4, um bloco de dados, m_1, com informação de uma mensagem, vindo da camada imediatamente superior à Camada Física é mapeado em símbolos e processado pelo bloco Processamento2. Esse mapeamento e esse processamento seguem a mesma lógica dos descritos anteriormente para o vetor de inicialização. O sinal resultante do processamento em questão é submetido, em conjunto com o sinal encriptado por E_1, à Operação Sinal-IV (OSIV). Idealmente, essa operação deve ser equivalente a um *one-time pad* (OTP) no domínio digital. Um possível exemplo dessa operação é a soma de fases. De fato, se as fases do sinal referente a m_1 forem somadas a fases aleatória e uniformemente distribuídas no intervalo $[0, 2\pi)$, as fases do sinal na saída da OSIV não trarão nenhuma informação sobre as fases do sinal referente a m_1.

[061] Opcionalmente, o sinal na saída da OSIV pode ser submetido a um novo Algoritmo de Encriptação de Sinal2, E_2, e a um novo processamento pelo bloco Processamento2. O algoritmo E_2 pode aprimorar algum aspecto desejável de segurança e não precisa, necessariamente, satisfazer os mesmos requisitos de E_1. O bloco de Processamento3 segue a mesma lógica descrita para os blocos de Processamento1 e 2.

[062] Os algoritmos E_1 E_2 , D_1 e D_2 são arbitrários, mas devem garantir que os sinais em sua saída sejam “suficientemente distintos” mesmo quando o contador do vetor de inicialização for alterado por um único bit. Uma possível maneira de avaliar se esses sinais são “suficientemente distintos” é convertê-los para o domínio binário e checar se houve difusão. Para satisfazer essa propriedade, pode ser necessário que E_1 opere com vários rounds de encriptação.

[063] A seguir, o sinal é transmitido por um conversor digital analógico (*digital to analog converter,* DAC), originando o sinal encriptado c_1. Esse sinal pode ser transmitido por um canal banda-base até o transmissor ou, se necessário, modular uma portadora para ser transmitido por um canal de banda passante. Essas portadoras podem estar, por exemplo, no intervalo de rádio-frequência (RF), de micro-ondas (microwaves, MW) ou óptico.

[064] Conforme mostra a Figura 4(b), o procedimento descrito anteriormente pode ser repetido para um *i*-ésimo vetor de inicialização, IV_i (β_1), (cujo contador fica ajustado para a posição *i*-1) em conjunto com um *i*-ésimo bloco, m*i*, com as mesmas chaves k_1 e k_2 aplicadas a E_1 e E_2, respectivamente. A reutilização dessas chaves permite a paralelização da encriptação de diversos blocos, em acordo com o número de processadores disponível, sendo uma grande vantagem do método proposto.

[065] A desencriptação do sinal segue a maioria dos passos da encriptação e está ilustrada na Figura 5. As diferenças entre os processos de desencriptação e de encriptação são as seguintes: (i) Os algoritmos de desencriptação de sinais, D_1 e D_2, substituem os algoritmos de encriptação de sinais, E_1 e E_2, respectivamente. Os algoritmos de desencriptação devem, a partir de suas chaves criptográficas,

compensar as operações realizadas por seus pares de encriptação; (ii) O sinal c*i* (*i*= 1, ..., N_m) substitui a entrada mi (i= 1, ...□, N_m) o bloco de Processamento2; e, (iii) Ao final do processo de desencriptação, um bloco de mapeamento de símbolos e conversão para bits, substitui o DAC do processo de encriptação, gerando, idealmente, os blocos transmitidos m*i* (*i*= 1, ..., N_m).

[066] Os diagramas de bloco das Figuras 4 e 5 não devem ser encarados de maneira restritiva. Por exemplo, é possível acrescentar um bloco de processamento entre os blocos de OSIV e D_2 na Figura 5 sem que haja um correspondente na Figura 4. Alterações do tipo não alteram o teor da proposta.

[067] Nota-se ainda que, como apresentado, a aplicação do método é direta para sinais de portadora única. Mas o método também pode ser aplicado para sinais de múltiplas portadoras, como é o caso daqueles que usam a tecnologia de multiplexação por divisão de frequências ortogonais (orthogonal frequency division multiplexing, OFDM). Neste caso, seria possível, por exemplo, usar o esquema proposto para encriptar os sinais que modulam cada subportadora OFDM. Alternativamente, a encriptação poderia ser feita sobre sinais que modulam um conjunto de subportadoras OFDM, causando, por exemplo, um embaralhamento das amostras desses sinais. Em outra alternativa, os sinais modulados nas subportadoras poderiam ser encriptados. Dada a inviabilidade de se elencar todas as possibilidades, destaca-se novamente que os diagramas de bloco das Figuras 4 e 5 não devem ser encarados de maneira restritiva.

[068] Assim, o método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, objeto da presente invenção, compreende as etapas de encriptação e desencriptação, onde:

[069] A encriptação, encripta a informação de um vetor de inicialização que contém um contador, processados na Subcamada de Codificação (SC) que mapeia o vetor de inicialização IV_1 em símbolos de sinais, ditos símbolos sendo referentes ao equivalente complexo em banda-base de um sinal com modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM) de ordem M arbitrária (M-QAM),

onde opcionalmente, esses símbolos podem ser processados pelo bloco Processamento1, na própria SC ou na Subcamada Dependente do Meio (SDM); onde o processamento pode ser na SC por embaralhamento de símbolos , ou na SDM por limitação de banda do sinal por meio de filtragem ocorrendo no domínio do tempo, no domínio da frequência ou em ambos. A seguir, o sinal processado é submetido ao Algoritmo de Encriptação de Sinal1, E_1, que também é alimentado com a Chave1, k_1. Em seguida o Sinal1 é mapeado em símbolos e processado pelo bloco Processamento2. Esse mapeamento e esse processamento seguem a mesma lógica dos descritos anteriormente para o vetor de inicialização IV_1. O sinal resultante do processamento em questão é submetido, em conjunto com o sinal encriptado por um algoritmo E_1, à Operação Sinal-IV (OSIV). Opcionalmente, o sinal na saída da OSIV pode ser submetido a um novo Algoritmo de Encriptação de Sinal2, E_2, e a um novo processamento pelo bloco Processamento2 da mesma maneira que o Processamento1;

[070] A desencriptação, desencripta a informação do Sinal processado, de forma semelhante à encriptação, onde: os algoritmos de encriptação de sinais, E_1 e E_2 são substituídos pelos algoritmos de desencriptação de sinais, D_1 e D_2, respectivamente, que compensam as operações realizadas por seus pares de encriptação a partir de suas chaves criptográficas. O sinal ci (i= 1, ..., Nm) substitui a entrada mi (i= 1, ..., Nm) o bloco de Processamento2 e ao final do processo de desencriptação, um bloco de mapeamento de símbolos e conversão para bits, substitui o DAC do processo de encriptação, gerando, os blocos transmitidos mi (i= 1, ..., Nm).

EXEMPLO DE APLICAÇÃO

[071] 1. Normalmente, os algoritmos de encriptação de sinais apresentados na literatura contam com até três estágios de encriptação, sendo que:

(i) Esses estágios realizam apenas operações lineares, como codificação de fase no domínio do tempo ou da frequência, embaralhamento de amostras no domínio do tempo ou da frequência e/ou adição de ruído gerado artificialmente;

(ii) Esses estágios são implementados em apenas um round, oferecendo apenas uma capacidade de difusão e/ou confusão limitada; e

(iii) Para elevar a difusão e a confusão do processo de encriptação, conforme explicado em outros pontos desta Invenção, cada bloco é encriptado com uma chave distinta, chamada de chave de bloco. A chave usada para encriptar o i-ésimo bloco é calculada a partir de parâmetros usados para determinar as chaves anteriores.

[072] O método proposto é baseado em um paradigma distinto que:

(i) Aplica as mesmas chaves para todos os blocos;

(ii) Utiliza uma estratégia similar ao modo de operação CTR usado em criptografia de dados; e

(iii) Requer que o algoritmo de encriptação ofereça um elevado nível de difusão e confusão.

[073] Para atingir estes objetivos e exemplificar a possibilidade de implantação prática, cria-se um algoritmo de encriptação de sinais, E_1, que replica algumas características do AES. Como esse algoritmo atua sobre sinais, nós o chamamos de s-AES.

[074] A criptografia de sinais em banda-base é baseada em algoritmos de DSP e exige operações com amostras de sinais discretos. Como as amostras podem ser caracterizadas por uma amplitude e uma fase, as operações da criptografia de sinais devem atuar sobre a amplitude, sobre a fase ou sobre a amplitude e sobre a fase dessas amostras.

[075] A Figura 6 mostra diagramas de bloco para as implantações do AES e do s-AES. No segundo desses algoritmos, uma mensagem m é dividida em blocos de 125 símbolos referentes a sinais complexos em banda-base. Estipula-se o uso de duas amostras por símbolo1. As amostras são, a seguir, submetidas a uma transformada rápida de Fourier (fast Fourier trasnform, FFT) e transmitidas por um filtro cosseno levantado (raised cosine filter, RCF) com fator de decaimento (roll-off) de 2.4%. Isso gera um total de 128 amostras espectrais não-nulas. Observa-se que o comprimento

de 125 bits do bloco de entrada foi calculado justamente para que, com uma taxa arbitrada em 2 amostras por símbolo e um roll-off baixo obtivessem-se 128 amostras na entrada do s-AES. Isso permite que assim como o AES, o s-AES também opere sobre blocos de 128 unidades de informação. Essa foi a primeira de várias analogias estabelecida entre o s-AES e o AES.

[076] Exemplos de sinais que podem ser usados são as versões em banda-base de sinais com chaveamento por desvio de fase binário (binary phase-shift keying, BPSK), chaveamento por desvio de fase em quadratura (quadrature phase-shift keying, QPSK) ou modulação de amplitude em quadratura (quadrature amplitude modulation, QAM) com 16 símbolos, 16-QAM.

[077] Outras analogias morfológicas e funcionais foram consideradas. Antes de apresentá-las, porém, cabe enfatizar que essas analogias foram baseadas em alguns critérios julgados convenientes. Outros critérios poderiam ser adotados e, também, poderiam conduzir a resultados satisfatórios do ponto de vista de segurança e de propagação dos sinais encriptados. As analogias apresentadas a seguir são, então, um ponto de partida para o estabelecimento de estratégias de criptografia de sinais e poderão ser aprimoradas. As analogias morfológicas estão indicadas na Tabela 1.

Tabela 1. Equivalência morfológica entre o s-AES e o AES.

AES	S-AES
Unidade de Informação: Bit	Unidade de Informação: Fase da Amostra
Byte: conjunto de 8 bits	S-Byte: Conjunto de fases de 8 amostras
Blocos: conjuntos de 16 bytes	S-Blocos: Conjunto de 16 s-bytes
Chaves compostas por 128 bits	S-Chaves compostas por fases de 128 amostras

[078] Em particular:

1. A unidade de informação no s-AES é a fase de cada amostra do sinal. Essa unidade de informação é tida como análoga à unidade de informação do AES, que é o bit;
2. Cada grupo de 8 amostras é visto como um “byte de sinal”, chamado de s-byte no s-AES, e análogo ao byte considerado no AES; e
3. Cada grupo de 8 s-bytes é visto como um “bloco de sinal”, chamado de s-bloco no s-AES, e análogo ao bloco considerado no AES;
4. Assim como um bloco do AES é organizado em uma matriz de 4x4 bytes para que os devidos processamentos ocorram, um s-bloco é organizado em uma matriz com as fases de 4x4 s-bytes;
5. As chaves usadas em cada round do s-AES também são formadas por uma matriz de 4x4 p-bytes. Essas chaves são chamadas de p-chaves.

[079] A primeira analogia funcional é relativa à operação AddRoundKey. No AES, essa operação é um XOR entre unidades de informação de uma chave e unidades de informação de um dado bloco. Por se tratar de uma situação binária, as unidades de informação são os bits ‘0’ e ‘1’. Para o XOR, há quatro combinações possíveis de entrada 00, 01, 10 e 11 e duas saídas possíveis e equiprováveis ‘0’ e ‘1’.

[080] No s-AES, as unidades de informação são fases que podem ter qualquer valor no intervalo $[0, 2\pi)$. Deve-se encontrar uma operação s-XOR que produza um efeito similar ao XOR binário, ou seja, o s-XOR deve operar sobre um par de fases de entrada e gerar uma fase de saída. Assim como as fases de entrada, as fases de saída do s-XOR devem estar no intervalo $[0, 2\pi)$. Além disso, qualquer fase de saída, $\emptyset o$, em um intervalo infinitesimal $d\emptyset$, $\emptyset o - d\emptyset/2 < \emptyset o < \emptyset o + d\emptyset/2$, deve ocorrer com probabilidade diferencial $d\emptyset/(2\pi)$. Uma operação simples que satisfaz essas propriedades é a soma das fases de entrada em módulo 2π. Assim, no s-AES a operação AddRoundKey é substituída pela soma das fases de uma s-chave com um

s-bloco, ambos dispostos em uma matriz de 4x4 s-bytes. Essa operação é aqui designada por s-AddRoundKey.

[081] Seguindo essa analogia, observa-se que uma maneira de se fazer um OTP entre dois sinais, um s-OTP, é, simplesmente, somar a fase de ambos. Esse resultado é importante e será utilizado nesta Invenção.

[082] A operação de ShiftRows lida apenas com posições dos bytes e não requer adaptações algébricas. No entanto, a aplicação das operações SubBytes, MixColumns e de expansão de chaves requer uma nova analogia funcional. Essa analogia consiste em um mapeamento entre fases, cujos valores variam continuamente em [0, 2π), e bits, '0' e '1'. Na versão atual do s-AES fez-se o seguinte mapeamento:

(a) Se a fase de uma amostra está em [0, π) ou em [π, 2π) atribui-se a essa amostra, respectivamente, um bit 0 ou 1. Com isso, cada s-byte é convertido a um byte;

(b) As operações de SubBytes, MixColumns e KeyExp são realizadas conforme a álgebra de GF(28) sobre os respectivos bytes; e

(c) O resultado dessas operações é convertido para um s-byte somando-se, em mod (2π), 0 ou π às fases das amostras consideradas em (a) quando o bit na posição correspondente àquela amostra for 0 ou 1, respectivamente.

[083] Por exemplo, se as fases de um s-byte são sBi= {0,2π; 0,5π; 0,3π ; 1,2π ; 1,5π ; 0,4π ; 0,7π; 1,7π}, a conversão estabelecida em (a) levará a um byte Bi= {0; 0; 0; 1; 1; 0; 0; 1}. Se as operações de SubBytes, MixColums ou KeyExp realizadas em GF(28) sobre Bi resultarem em Bo= {1; 0; 1; 1; 0; 0; 1; 0}, o s-Byte resultante desse processo será: sBo= sBi+{ π; 0; π; π; 0; 0; π ; π }= {1,2π; 0,5π ; 1,3π; 0,2π; 1,5π; 0,4π; 1,7π; 0,7π}.

[084] Em analogia a outras nomenclaturas usadas neste documento, as operações AddRoundKey, ShiftRows, SubBytes, MixColumns e KeyExp, adaptadas ao paradigma do s-AES serão, de agora em diante, designadas, respectivamente, por s-AddRoundKey, s-ShiftRows, s-SubBytes, s-MixColumns e s-KeyExp.

[085] Ao final de todas as operações, o sinal é reconvertido para o domínio do tempo, modulado em uma portadora e propagado até o receptor autorizado por meio de um certo canal de comunicação. O receptor autorizado deve demodular o sinal criptografado e desencriptá-lo por meio de uma s-chave que usa o complexo conjugado das fases utilizadas na s-chave de encriptação.

[086] No modo de Operação de Sinais, simulações com esse modelo foram bem-sucedidas na situação back-to-back, isto é, quando o transmissor está diretamente conectado ao receptor. No entanto, ao inserir-se um canal banda-base com ruído aditivo, branco e gaussiano (additive, white, and Gaussian noise, AWGN), verificou-se que não era possível recuperar o sinal criptografado mesmo quando a relação sinal-ruído era bastante alta, por exemplo, 30 dB.

[087] Verificou-se, que as operações de s-AddRoundKey, s-ShiftRows e s-Key-Exp não eram comprometidas pelo canal AWGN. No entanto, as operações s-SubBytes e s-MixColumns eram afetadas por esse canal. De fato, essas operações realizam transformações lineares (s-MixColumns) e não-lineares (s-SubBytes) sobre as fases do sinal de entrada. Essas transformações dependem apenas dos valores dessas fases de entrada. Quando não há ruído, as transformações realizadas no transmissor podem ser desfeitas pelo receptor. Mas quando há ruído, o valor das fases de entrada é alterado de tal forma que as transformações não podem mais ser desfeitas.

[088] Para resolver este problema, decidiu-se utilizar um análogo do modo de operação CTR para garantir a aleatoriedade da encriptação do s-AES. A aplicação de modos de operação nunca foi realizada em criptografia de sinais e a utilização desse esquema é uma inovação importante de nossa proposta. A versão do CTR para criptografia de sinais é chamada de s-CTR.

[089] Conforme indica a Figura 7, no esquema do s-CTR, o s-AES deixa de atuar sobre o sinal que será transmitido pelo canal. Nessa situação, o s-AES atua sobre as amostras do sinal de um *nonce* e gera um conjunto de fases que é usado para fazer um s-OTP com o sinal da mensagem que será encriptada. Isso implica que, de forma direta, o sinal a ser encriptado:

a. Não está sujeito às operações s-SubBytes e s-MixColumns, responsáveis pela penalidade de ruído relatada anteriormente; e

b. É submetido a uma operação s-AddRoundKey, que não introduz penalidades na presença de ruído. Se o s-AES tiver sido bem projetado, essa operação de s-AddRoundKey terá um efeito similar a um s-OTP, capaz de produzir segurança perfeita.

[090] Essas observações indicam que o sinal criptografado pode ser transmitido por um canal AWGN sem penalidades expressivas.

[091] A solução final contempla dois passos adicionais aos descritos até o momento. O primeiro desses passos está relacionado com o fato de que as amostras de sinais são caracterizadas por uma amplitude e por uma fase. A descrição anterior do s-AES contempla apenas a utilização da fase. Então, para envolver a amplitude em nossa solução, após os rounds análogos ao AES, o s-AES conta com uma operação de permutação de amplitudes, s-Permut.

[092] Para não depender de uma chave adicional, a operação s-Permut dispõe as fases do sinal na saída do último round do s-AES, φi, em ordem crescente e permutam-se as amplitudes, A_i, das amostras em acordo com o índice das fases nessa ordenação. Para explicar esse procedimento, considera-se um exemplo hipotético em que o s-bloco possui apenas 4 amostras e que essas quatro amostras após o processamento do último round do s-AES são caracterizadas por amplitudes A_i e fases φi ($i= 1, ..., 4$), tais que: $\{(A1; \varphi1), (A2; \varphi2), (A3; \varphi3), (A4; \varphi4)\}= \{(0,2; 150º), (0,5; 10º), (0,3; 40º), (0,8; 25º)\}$. O ordenamento crescente das fases leva a: $\varphi2 = 10º < \varphi4 = 25º < \varphi3 = 40º < \varphi1 = 150º$. Seguindo os índices das fases, tem-se: 2, 4, 3, 1. Assim, após a operação s-Permut, as amostras serão {(0,5; 150º), (0,8 ; 10º), (0,3; 40º), (0,2; 25º)}.

[093] O segundo passo adicional está relacionado com a informação espectral do sinal. Se a densidade espectral de potência (power spectral density, PSD) do sinal variar com a frequência, um espião que tente fazer um ataque de força bruta pode concentrar seus esforços nas amostras que estão nas regiões espectrais cuja PSD é

maior. Assim, é conveniente que a PSD seja a mais plana possível e, por isso, utiliza-se um RCF com fator de roll-off r reduzido. No entanto, na região de roll-off a amplitude da PSD é reduzida. Apesar de essa região ser estreita, deseja-se impor a maior dificuldade possível aos ataques dos espiões. Então, nossa proposta é adicionar um sinal, equivalente a um ruído passa-alta, a essas regiões para aplanar a PSD do sinal encriptado. Para isso, após a transmissão pelo RCF, as amplitudes de todas as amostras que residem na região espectral de roll-off são acrescidas à N(f)= C- C·HRCF(f , em que f é a frequência, HRCF(f) é a função de transferência associada ao RCF e C é a amplitude média das amostras do sinal, que não estão na região de roll-off. Na detecção do sinal, tanto um receptor autorizado como um espião podem medir o valor de C para retirar a contribuição de N(f). No entanto, como as amplitudes da amostra do sinal encriptado estão permutadas, apenas o receptor autorizado é capaz de retirar as contribuições de N(f) nas amostras apropriadas.

[094] A Figura 8 mostra um diagrama de blocos do exemplo considerado para o método proposto. As operações internas do s-AES e dos blocos de processamento também são mostradas.

[095] São apresentados os principais resultados obtidos para a implantação da combinação s-AES/ s-CTR, que constitui o exemplo da técnica proposta considerado neste anexo. Em particular foram realizados testes referentes à envoltória complexa em banda-base de sinais com chaveamento por desvio de fase binário (binary phase-shift keying, BPSK), com chaveamento por desvio de fase em quadratura (quadrature phase-shift keying, QPSK) e com modulação por quadratura de amplitude de 16 níveis (16 quadrature amplitude modulation, 16-QAM). A taxa de símbolo de todos esses sinais é de 28 GBaud e a banda deles é limitada por um RCF com fator de roll-off de 2.4%.

[096] São mostrados os resultados dos testes relativos à envoltória complexa em banda-base de sinais 16-QAM (o sinal mais complexo entre os três abordados). No entanto, é importante mencionar que resultados similares foram obtidos para as envoltórias complexas em banda-base de sinais BPSK e QPSK.

[097] A partir de agora, as envoltórias complexas em banda-base dos sinais BPSK, QPSK e 16-QAM serão identificadas, respectivamente, por BPSK*, QPSK* e 16-QAM*. Em muitas de nossas análises, um sinal de entrada não encriptado é submetido ao s-AES/s-CTR e, posteriormente, é desencriptado. Designar-se-ão (*i*) o sinal de entrada, não encriptado, por NE, (*ii*) o sinal encriptado pelo s-AES por E e (*iii*) o sinal encriptado e desencriptado por ED.

[098] A apresentação dos resultados é feita em três partes. Mostram-se os resultados da aplicação da técnica em uma configuração back-to-back, onde as avaliações têm por objetivo verificar se os resultados esperados foram atingidos e testar a consistência desses resultados. São considerados os resultados referentes à propagação dos sinais encriptados por canais AWGN e óptico. Por fim, são consideradas as avaliações numéricas em relação à segurança imposta pelo s-AES.

Configuração Back-to-back

[099] A Figura 9 ilustra os espectros de sinais 16-QAM* NE ((a)-(c)), E ((d)-(f)) e ED, ((g)-(i)). As Figuras 9(a), (d) e (g) mostram espectros de amplitude referentes à média de 500 sinais. Observa-se que as amplitudes dos sinais NE 9(a) e DE 9(g) são muito similares, indicando o sucesso da desencriptação. Além disso, os espectros de amplitude de NE e ED ocupam uma banda de ~14,34 GHz com uma região de decaimento de amplitudes entre 14,00 e 14,34 GHz criada pelo RCF. Por outro lado, como esperado, as amplitudes do espectro do sinal E 9(b) são diferentes daquelas observadas para os sinais NE e ED. Isso é uma decorrência da operação s-Permut. Nota-se que o espectro do sinal também ocupa uma banda de ~14,34 GHz. No entanto, a adição do ruído passa-alta N(f) tornou plano o espectro do sinal E (sem a região de decaimento de amplitudes entre 14,00 e 14,34 GHz observada para os sinais NE e ED). Isso mostra que a estratégia adotada realmente faz com que o sinal encriptado assemelhe-se a um ruído branco.

[100] As Figuras 9(b), (e) e (h) mostram os espectros de fase referentes aos espectros de amplitude das Figuras 9(a), (d) e (g), respectivamente. Assim como ocorreu para as amplitudes, nota-se que as fases dos sinais NE e ED são similares

entre si, mas diferem substancialmente daquelas associadas ao sinal E. Essas semelhanças e diferenças devem ser observadas não apenas para a média dos 500 sinais, mas também para sinais individuais. Para mostrar que isso realmente ocorre, ilustra-se nas Figuras 9(c), (f) e (i), os espectros de fase referentes a um único sinal. Uma vez mais, as semelhanças entre as fases associadas os casos NE e ED, bem como a diferença entre as fases desses casos com aquelas do sinal E são constatadas.

[101] A Figura 10 exibe as constelações de sinais 16-QAM* a) NE, b) E e c) ED. Corroborando os resultados espectrais, observa-se que as constelações associadas aos sinais NE e ED são similares e apresentam 16 símbolos bem definidos. Por sua vez, a constelação relativa ao sinal E apresenta-se difusa e sugere (como será visto posteriormente) uma BER bastante elevada, como esperado para um sinal encriptado.

[102] As Figuras 11 e 12 mostram os histogramas para as distribuições de amplitude e de fase dos sinais NE, E e DE. As distribuições verificadas para os sinais NE (11(a) e 12(a)) e DE (11(c) e 12(c)) são aquelas previstas para um sinal 16-QAM* e dispensam mais comentários. O inset da Figura 11(b) sugere que as distribuições de amplitude dos sinais E nos eixos I e Q são gaussianas e a Figura 12(b) indica que a distribuição das fases do sinal E é uniforme. Quando essas duas características ocorrem simultaneamente, pode-se mostrar que as amplitudes do sinal (considerando simultaneamente as contribuições dos eixos I e Q) seguem uma distribuição de Rayleigh. Isso é verificado na curva principal da Figura 12(b).

[103] É importante notar que a criptografia realizada pelo s-AES impõe mudanças de fase e trocas de amplitude entre as amostras. Essas operações não devem alterar a energia do sinal processado, isto é, a energia do sinal E deve ser a mesma do sinal NE. Os diagramas de constelação permitem verificar esse fato, onde tem-se que a energia do sinal NE é $E_{NE}= [4(1^2+1^2)+8(1^2+3^2)+ 4(3^2+3^2)]/16= 10$ (un. arb.)^2. Como as componentes I e Q do sinal NE são independentes, a energia do sinal E é $E_E= \sigma^2= \sigma_I^2+ \sigma_Q^2$, em que σ_I^2 e σ_Q^2 são, respectivamente, as variâncias das componentes das

distribuições nos eixos I e Q. Os dados referentes ao inset da Figura 11(b) indicam que σ_I = aprox. σ_Q = aprox. 2,255 un. Arb. Assim, E_E= 10,17 (un. arb.)^2 = aprox. E_{NE}, como esperado.

[104] Os resultados obtidos e apresentados nas Figuras 9, 10, 11 e 12 confirmam o bom funcionamento do s-AES e a consistência das simulações.

[105] A Figura 13 mostra o desempenho de sinais E e ED quando há um canal AWGN entre o transmissor, que encripta o sinal pelo s-AES, e o receptor, que desencripta esse sinal. São considerados os sinais BPSK*, QPSK* e 16-QAM*. A BER do sinal E é constante e ~0.5 para qualquer razão sinal ruído (signal-to-noise ratio, SNR) e para qualquer dos 3 sinais. Essa é justamente a maior BER que um sistema de comunicação pode oferecer (Se a BER fosse, por exemplo, de 0,6 bastaria usar um inversor para reduzi-la a 0,4). Isso indica a dificuldade que um interceptador terá para recuperar o sinal NE a partir de E.

[106] Outro ponto importante é que o sinal E não experimenta nenhuma penalidade significativa em relação ao sinal NE. Isso faz sentido porque a estratégia proposta apenas altera as fases e permuta as amplitudes das componentes espectrais do sinal NE (convertendo-o no sinal E). Essas operações fazem que a distribuição de amplitude das amostras dos sinais E seja gaussiana e tenha valores superiores à do sinal NE, como ilustrado nas Figuras 10 e 11. Mas o aumento das amplitudes só prejudicará o desempenho dos sinais no caso de canais não-lineares.

[107] Também foi simulada a situação em que os sinais BPSK*, QPSK* e 16-QAM* foram modulados em uma portadora óptica de 193.1 THz e propagados por um conjunto de enlaces ópticos. Cada enlace foi constituído por:

(i) Uma fibra padrão de 80 km de comprimento, com atenuação de0,25 dB/km, dispersão de 16 ps/(nm·km), inclinação de dispersão de 0,08 ps/(nm2·km) e coeficiente não-linear de 10 (W·km)-1;

(ii) Um primeiro amplificador à fibra dopada com Érbio (Erbium doped fiber amplifier, EDFA) com ganho de 20 dB e figura de ruído (noise figure, NF) de 4.4 dB;

(iii) Uma fibra de compensação de dispersão (dispersion compensating fiber, DCF) com comprimento de 12,8 km, atenuação de 0,4 dB/km, dispersão de -100 ps/(nm·km), inclinação de dispersão de -0,50 ps/(nm2·km) e coeficiente não-linear de 10 (W·km)-1, e (iv) Um segundo EDFA com ganho de 5,12 dB e NF= 4.4 dB.

[108] Os parâmetros das fibras são válidos para 193,1 THz. A propagação pela fibra foi simulada a partir da solução da equação não linear de Schrödinger pelo método de split-step Fourier realizada no software VPITransmissionMaker™. De fato, nessa etapa foi realizada uma cossimulação entre o Matlab™ (encriptação e desencriptação a partir do código do s-AES desenvolvido por nossa equipe) e o VPITransmissionMaker™ (modulação, propagação e demodulação do sinal E).

[109] A Figura 14 ilustra as curvas de BER em função da distância de propagação, L. Essas curvas foram obtidas após a otimização das potências dos sinais BPSK, QPSK e 16-QAM propagados pela fibra. Nota-se, agora que os sinais ED experimentam alguma degradação. Por exemplo, no limite da FEC, o alcance dos sinais 16-QAM é reduzido de 720 para 640 km.

[110] A fim de avaliar o motivo de tal degradação, anulou-se o coeficiente não-linear da fibra. Essa variação não afetou significativamente a BER dos sinais ED e isso descarta uma influência apreciável da auto-modulação de fase. A degradação observada é consequência de não-linearidades no modulador e/ou de ruídos elétricos não removidos e/ou do possível fato de os desempenhos de sinais E e NE serem otimizados para diferentes potências de lançamento na fibra.

[111] Para verificação da Segurança, realizaram-se simulações referentes ao efeito avalanche para avaliar a difusão provida pelo s-AES. Para isso, escolheu-se uma palavra de referência PR de comprimento n bits. Essa palavra foi encriptada e conduziu um texto cifrado de referência, CTR. A seguir, alterou-se o i-ésimo bit de PR, originando a palavra Pi, em que i= 1, ..., n. A encriptação de Pi gerou um bloco CTi cujos bits foram comparados com os de CTR.

[112] Em um exemplo hipotético para n= 4, poder-se-ia ter:

PR= 0111; CTR= 1101;

P1= 1111; CT1= 1100;

P2= 0011; CT2= 1011;

P3= 0101; CT3= 1110;

P4= 0111; CT4= 0000;

[113] Nesse caso, a comparação entre CTi e CTR indica que os bits desses textos cifrados diferem em 25%, 50%, 50% e 75% para i= 1, 2, 3 e 4, respectivamente, e que o valor médio dessa diferença é 50%.

[114] A Figura 15 mostra o histograma obtido para n = 250, sendo 125 bits para uma palavra associada ao sinal do eixo I e 125 bits para uma palavra referente ao sinal do eixo Q de um sinal 16-QAM*, e para 100 palavras chaves. Observa-se que, conforme desejado, o histograma segue uma distribuição gaussiana com média de 50%.

[115] Para avaliar se a dispersão dessa distribuição é aceitável, foi feita uma comparação com a mesma curva para o AES (100 palavras-chave de 128 bits). Observa-se que o desvio padrão do s-AES é ligeiramente menor que o do AES. Isso indica que uma possível implantação comercial do s-AES é vantajosa em termos da difusão.

[116] Adotando um procedimento similar ao da difusão, mas mantendo a mensagem fixa e alterando-se as palavras associadas à chave de encriptação, obteve-se a distribuição para a confusão ilustrada na Figura 15. Novamente, observa-se uma distribuição gaussiana com valor médio de 50% e desvio padrão inferior àquele oferecido pelo AES. Assim, a adoção do s-AES também é vantajosa sobre a do AES em termos da confusão.

[117] Para avaliar a aleatorização provida pelo s-AES, encriptou-se uma palavra de referência, PR, com uma chave de referência, CR, obtendo um texto cifrado CT1. A seguir, aplicou-se o modo de operação s-CTR, proposto nesse projeto, para encriptar PR com CR. Apesar de a mensagem e a chave criptográfica serem as mesmas, o modo de encriptação altera o texto cifrado que, agora é chamado de CT2. Procedeu-

se dessa maneira até a obtenção do texto cifrado CTn e compararam-se os valores de todos os CTi entre si.

[118] Em um novo exemplo hipotético com n= 4, poder-se-ia ter:

PR= 0111; CR= 0101; CT1= 1101;

PR= 0111; CR= 0101; CT2= 0001;

PR= 0111; CR= 0101; CT3= 1001;

PR= 0111; CR= 0101; CT4= 1000;

[119] Assim, comparando-se o número de bits diferentes entre CTi e CTj (i= 1,..,, 4; j= 1,...,4), obtém-se uma matriz Hermitiana real com elementos diagonais nulos.

$$\rho_{ij} = \begin{bmatrix} 0 & 0,50 & 0,25 & 0,50 \\ 0,50 & 0 & 0,25 & 0,50 \\ 0,25 & 0,25 & 0 & 0,25 \\ 0,50 & 0,50 & 0,25 & 0 \end{bmatrix}$$

[120] A Figura 16 mostra, em um gráfico 3D os valores de *P*ij para n= 250 e 100 palavras de referência. Para i diferente de j, *P*ij tem um valor médio de 0,50. Isso indica que a utilização do s-AES com o s-CTR para encriptar a mesma mensagem com a mesma chave criptográfica fará que, em média, 50% dos bits dos sinais cifrados difiram entre si em encriptações sucessivas. Esse resultado, indica que o s-AES também atende os requisitos de aleatoriedade da encriptação.

[121] Outra métrica importante é a robustez à ataques de força bruta. Como o s-AES altera a fase e a posição de cada amostra, ambos esses fatores influenciarão em tal robustez. Nossa análise inicia-se com a robustez às alterações de fase causadas pelo s-AES, supondo que a operação s-Permut não é implantada.

[122] Nessa situação, a amplitude de todas as amostras é preservada, mas a fase θ_i da i-ésima amostra é deslocada por um valor X_i resultante da aplicação do s-AES. Assim, um interceptador receberá um sinal cujas amostras têm fase $\theta_i + X_i$ e, em princípio, deveria conhecer o valor exato de X_i para subtraí-lo de ($\theta_i + X_i$) e recuperar o sinal apropriadamente. No entanto, o interceptador pode errar no valor de X_i, atribuir

à i-ésima amostra uma fase $\theta_i + \Delta\theta_i$ e ainda assim recuperar o sinal dentro do limite da FEC. É necessário então, estimar qual é o limite aceitável para Δθi para cada tipo de sinal.

[123] Para fazer essa estimativa, realizaram-se simulações com a suposição de que o erro Δθi fosse uma variável aleatória uniformemente distribuída entre - Δθ e Δθ. Assim, por exemplo, se Δθ = 10º, então a fase atribuída à i-ésima fatia é uma variável aleatória uniformemente distribuída no intervalo θi $\pm$ 10º. Nota-se que essas simulações são referentes à perspectiva de um interceptador ilegal. Os resultados estão apresentados na Figura 17. Cada ponto corresponde à média de 3000 simulações para um dado valor de Δθ para FEC de $2x10^{-3}$ adotada nesta invenção, os valores limites de Δθ são ~ 45º, 33º e 15º, respectivamente, para sinais BPSK*, QPSK* e 16-QAM*.

[124] A máxima diferença entre dois valores da variável aleatória θi $\pm$ Δθi é 2 Δθ (= θi + Δθ -(θi $\pm$ Δθ)) e o valor médio dessa variável é Δθ. Assim, para descobrir a fase de cada amostra, o interceptador terá que realizar, em média, (360º / Δθ) tentativas, em que Δθ é expresso em graus. Para acertar as n_s amostras por bloco, o interceptador precisará, então de

$$N_f = \left(360/\Delta\theta\right)^{n_s}$$

tentativas. Como cada s-bloco tem n_s= 128 amostras, $N_f \underline{\sim} 8^{ns} = 3{,}9x10^{115}$, $10{,}9^{ns} \underline{\sim} 6{,}2x10^{132}$ e $24^{ns} \underline{\sim} 4{,}6x10^{176}$, respectivamente, para os sinais BPSK*, QPSK* e 16-QAM*. O número de tentativas necessárias para quebrar o AES-256 é $2^{256} \underline{\sim} 1{,}1x10^{77}$. Logo, para o pior caso de sinais BPSK*, a robustez a ataques de força bruta provida pelo s-AES é 38 ordens de grandeza maior que a do AES-256, usado para encriptar mensagens ultrassecretas. Essa diferença refere-se apenas à análise de fase.

[125] Considera-se agora, a robustez em relação à amplitude da operação s-Permut.

[126] Supõe-se agora que o interceptador conhece, de alguma maneira, todas as fases das amostras. Em um conjunto de ns amostras, há ns! permutações possíveis. No entanto, o interceptador pode recuperar o sinal dentro do limite da FEC se as

amplitudes de um determinado número de amostras, N_{certas}, forem conhecidas. Assim, o número de permutações possíveis é reduzido para

$$N_a = \frac{n_s!}{(n_s - N_{certas})!}$$

[127] A Figura 18 mostra os resultados obtidos a partir de simulações para a BER em função de N_{certas}. Novamente, cada ponto corresponde à média de 3000 simulações. Para o limite considerado da FEC, nota-se que o interceptador precisa conhecer as amplitudes das amostras nas posições corretas para 66, 108 e 122 amostras para os casos dos sinais BPSK*, QPSK* e 16-QAM*, respectivamente. Assim, no limite da FEC, $N_a \simeq 1{,}2\text{x}10^{130}$, $\simeq 1{,}5\text{x}10^{197}$, $\simeq 5{,}3\text{x}10^{212}$, respectivamente, para os sinais BPSK*, QPSK* e 16-QAM*.

[128] No geral, o número de tentativas associadas à quebra da estratégia proposta por um ataque de força bruta será

$$N_{ataques} = N_f N_a = \left(\frac{360}{\Delta\theta}\right)^{n_s} \frac{n_s!}{(n_s - N_{certas})!}$$

[129] As curvas da Figura 19 mostram o log($N_{ataques}$) em função do número de amostras cujas amplitudes, fases e posições são exatamente conhecidas, Ncertas, para o caso em que a BER limite da FEC é atingida. Para obter essas curvas, estipulou-se um determinado valor de N_{certas} e ajustou-se $\Delta\theta$ para que a BER atingisse, aproximadamente, o limite de $2\text{x}10^{-3}$. Os valores de N_{certas} e $\Delta\theta$ foram, então, substituídos em (3) para obter $N_{ataques}$.

[130] Como nas Figuras 17 e 18, cada ponto da Figura 19 corresponde à média das simulações de 3000 s-blocos. Os resultados são válidos para sinais BPSK*, QPSK* e 16-QAM*.

[131] Observa-se que para o sinal BPSK* a dupla de valores (N_{certas} ~ 98, $\Delta\theta$ ~ 30,5º) minimiza $N_{ataques}$. Mas, mesmo nesse mínimo, $N_{ataques}$ é ~ 10^{320} e 243 ordens de grandeza superior ao necessário para quebrar o AES. Para valores inferiores a N_{certas}= 92, à medida que N_{certas} diminui, log($N_{ataques}$) aumenta monotonicamente. Nota-se que log(Nataques) tende a infinito nas proximidades de uma assíntota vertical em N_{certas}= N_{min}= 89. Isso indica que mesmo que o interceptador conheça as fases exatas de todas as amostras, só será possível recuperar o sinal dentro do limite da FEC se as amplitudes (e suas posições) de N_{min}= 89 amostras (~69,5% das 128 amostras) forem conhecidas.

[132] Para os sinais QPSK* e 16-QAM*, quando N_{certas} diminui, N_{ataque}s aumenta monotonicamente e os valores de N_{min} são, respectivamente, 97 (~75,7%) e 123 (~96%). Esses resultados sugerem que a utilização de modulações de ordem superior contribui significativamente para melhorar a segurança do processo de encriptação.

[133] O exemplo de aplicação da técnica proposta baseado na combinação do s-AES com o s-CTR. Todos os resultados obtidos mostraram-se adequados, destacando-se que:

(i) Conforme esperado, a BER dos sinais encriptados é de 0.5;

(ii) A combinação s-AES/ s-CTR mostrou-se superior ao AES em termos de difusão e confusão; e

(iii) A combinação s-AES/ s-CTR mostrou oferecer mais robustez a ataques de força bruta que o AES.

[134] Em criptografia de dados, os modos de operação são utilizados para aleatorizar a criptografia. Por outro lado, em criptografia de sinais, os modos de operação são necessários para evitar que os sinais, sujeitos à degradação do ruído do canal, sejam submetidos a algoritmos que realizam operações lineares e não-lineares cujo resultado depende de características do próprio sinal. Tal observação, é inédita na literatura e reforça não só o caráter inovador, mas também os desafios necessários para chegar à nossa proposta.

[135] Assim, pelas características de configuração e funcionamento, acima descritas, pode-se notar claramente que o MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA, trata-se de um novo método para o Estado da Técnica o qual reveste-se de condições de inovação, atividade inventiva e industrialização inéditas, que o fazem merecer o Privilégio de Patente de Invenção.

REIVINDICAÇÕES

1 - MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA, método para encriptar os sinais referentes a vários blocos com uma única chave criptográfica, relacionado à criptografia de sinais discretos realizados na Camada Física, ***caracterizado por*** criptografar sinais discretos de qualquer taxa de transmissão propagados por qualquer distância, ditos sinais referentes a vários blocos com uma única chave criptográfica; dito método o qual: (i) Aplica as mesmas chaves para todos os blocos; (ii) Utiliza uma estratégia similar ao modo de operação CTR usado em criptografia de dados; e (iii) Requer que o algoritmo de encriptação ofereça um elevado nível de difusão e confusão; dito método compreendendo as etapas de encriptação e desencriptação.

2 – MÉTODO, de acordo com a reivindicação 1, ***caracterizado por*** encriptar a informação de um vetor de inicialização que contém um contador, processados na Subcamada de Codificação (SC) que mapeia o vetor de inicialização IV1 em símbolos de sinais, ditos símbolos sendo referentes ao equivalente complexo em banda-base de um sinal com modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM) de ordem M arbitrária (M-QAM), onde opcionalmente, esses símbolos podem ser processados pelo bloco Processamento1, na própria SC ou na Subcamada Dependente do Meio (SDM); a seguir, o sinal processado é submetido ao Algoritmo de Encriptação de Sinal1, E1, que também é alimentado com a Chave1, k1; em seguida o Sinal1 é mapeado em símbolos e processado pelo bloco Processamento2; onde o mapeamento e o processamento seguem a mesma lógica para o vetor de inicialização IV1; onde o sinal resultante do processamento é submetido, em conjunto com o sinal encriptado por um algoritmo E1, à Operação Sinal-IV (OSIV).

3 – MÉTODO, de acordo com a reivindicação 2, ***caracterizado pelo*** processamento poder ser na SC por embaralhamento de símbolos, ou na SDM por limitação de

banda do sinal por meio de filtragem ocorrendo no domínio do tempo, no domínio da frequência, em ambos ou em combinações fracionárias de ambos.

4 – MÉTODO, de acordo com a reivindicação 2, ***caracterizado por*** opcionalmente, o sinal na saída da OSIV poder ser submetido a um novo Algoritmo de Encriptação de Sinal2, E2, e a um novo processamento pelo bloco Processamento2 da mesma maneira que o Processamento1.

5 – MÉTODO, de acordo com a reivindicação 1, ***caracterizado por*** desencriptar a informação do Sinal processado, de forma semelhante à encriptação, onde: os algoritmos de encriptação de sinais, E1 e E2 são substituídos pelos algoritmos de desencriptação de sinais, D1 e D2, respectivamente, que compensam as operações realizadas por seus pares de encriptação a partir de suas chaves criptográficas; O sinal ci (i= 1, ..., Nm) substitui a entrada mi (i= 1, ..., Nm) o bloco de Processamento2 e ao final do processo de desencriptação, um bloco de mapeamento de símbolos e conversão para bits, substitui o DAC do processo de encriptação, gerando, os blocos transmitidos mi (i= 1, ..., Nm).

6 – MÉTODO, de acordo com as reivindicações 2 e 5, ***caracterizadas pelos*** algoritmos E1, E2, D1 e D2 serem arbitrários, mas garantindo que os sinais em sua saída sejam “suficientemente distintos” mesmo quando o contador do vetor de inicialização for alterado por um único bit, podendo operar com vários rounds de encriptação.

7 – MÉTODO, de acordo com a reivindicação 6, ***caracterizado por*** criar um algoritmo de encriptação de sinais, E1, que replica algumas características do AES; Como esse algoritmo atua sobre sinais, nós o chamamos de s-AES.

8 – MÉTODO, de acordo com a reivindicação 2, ***caracterizado por*** alternativamente, a encriptação poder ser feita sobre sinais que modulam um conjunto de subportadoras OFDM.

9 – MÉTODO, de acordo com a reivindicação 2, ***caracterizado por*** alternativamente, a encriptação poder ser feita sobre sinais modulados nas subportadoras.

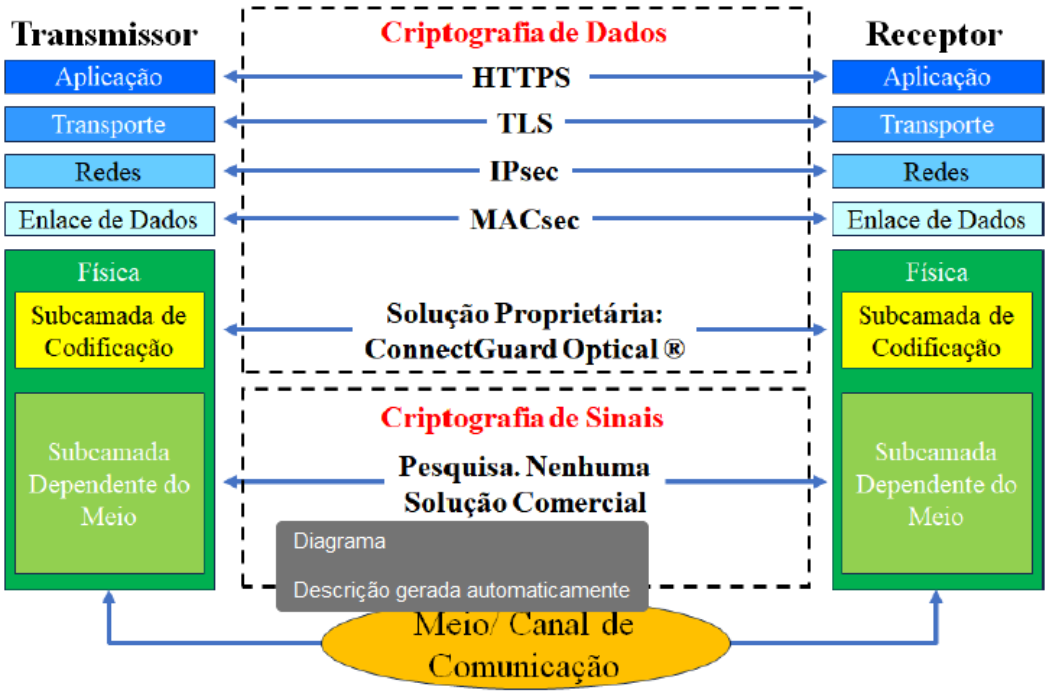

Figura 1

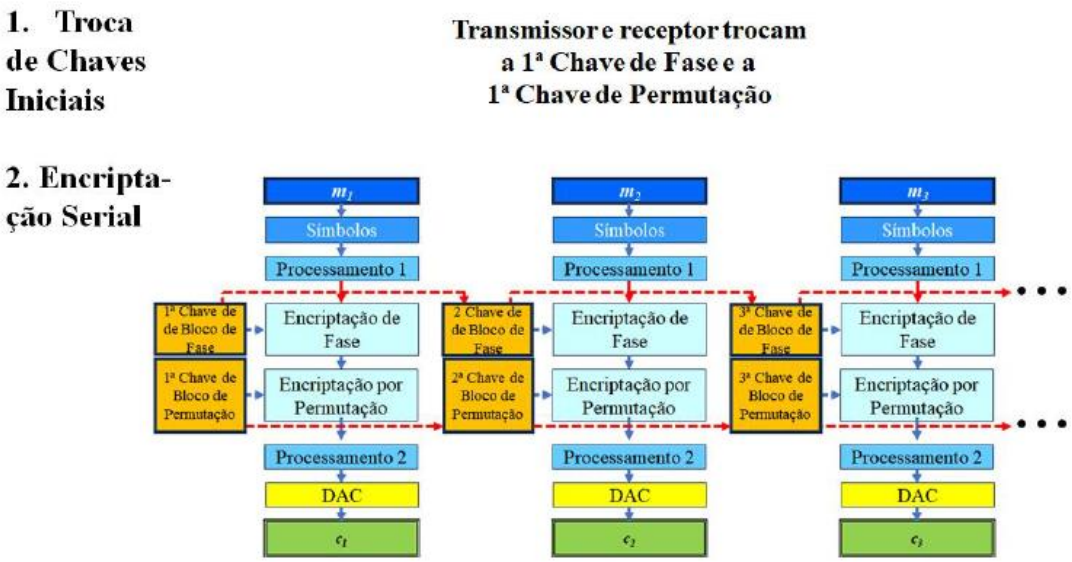

Figura 2

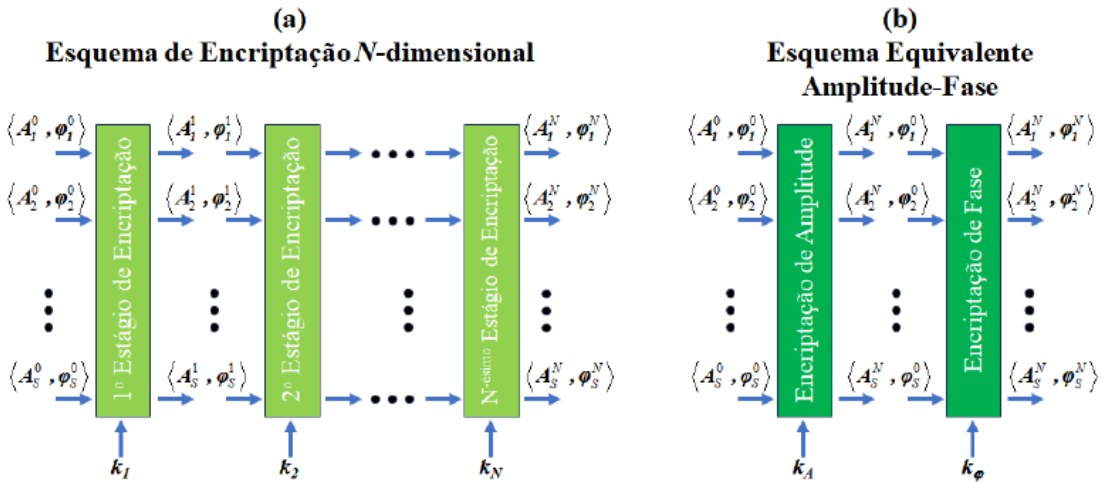

Figura 3

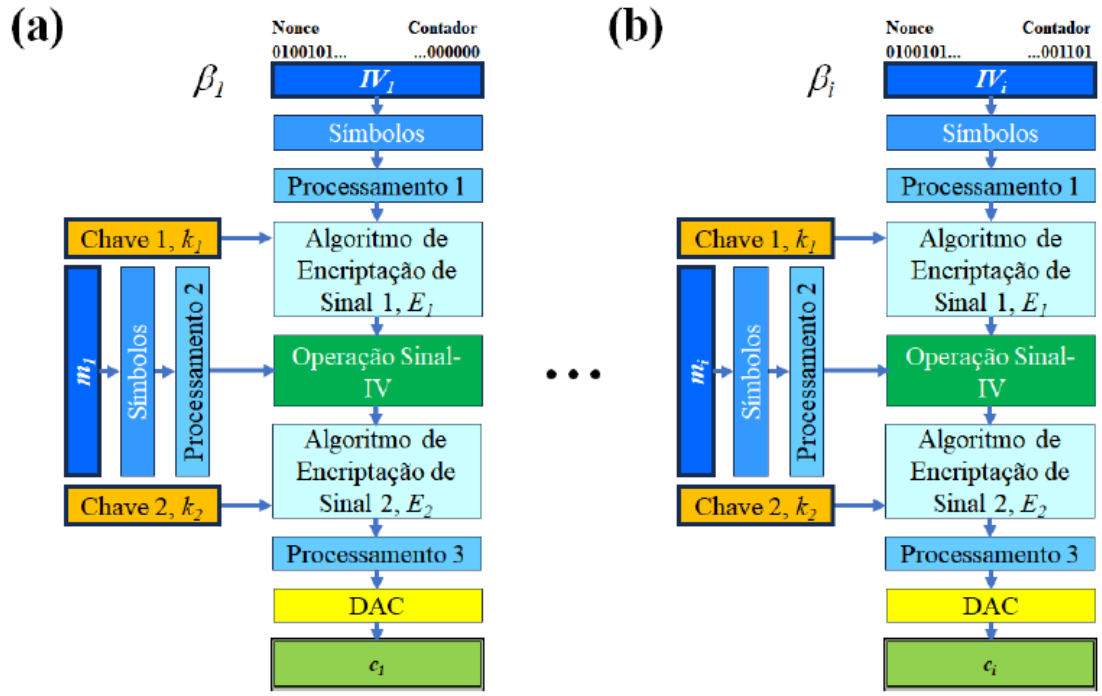

Figura 4

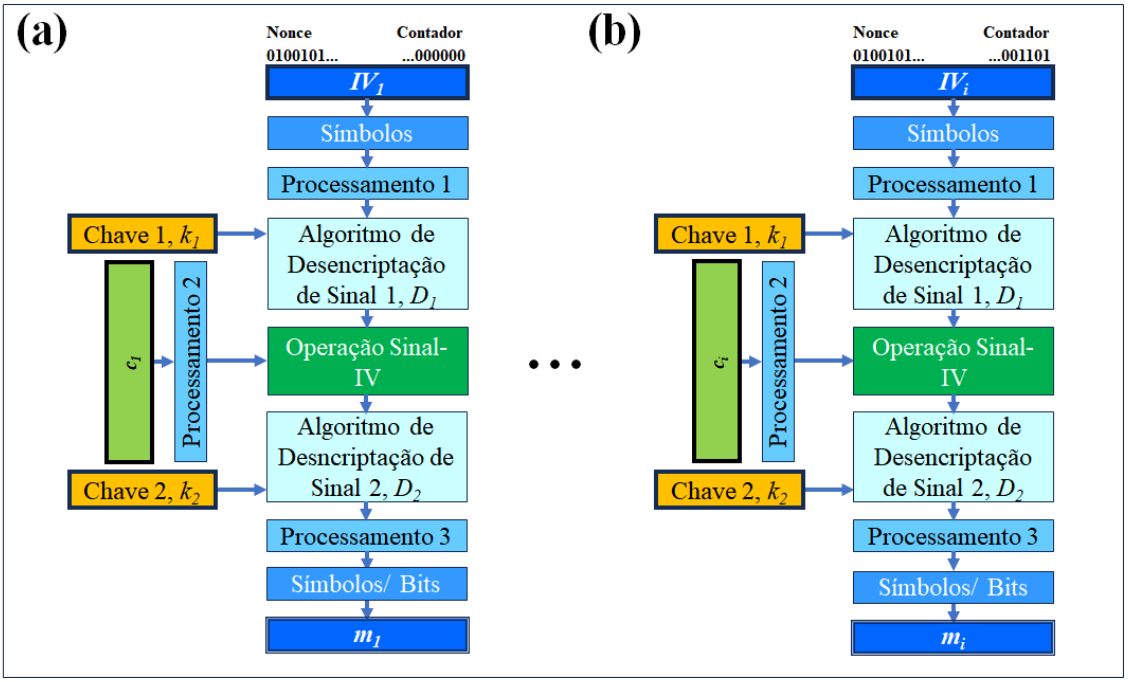

Figura 5

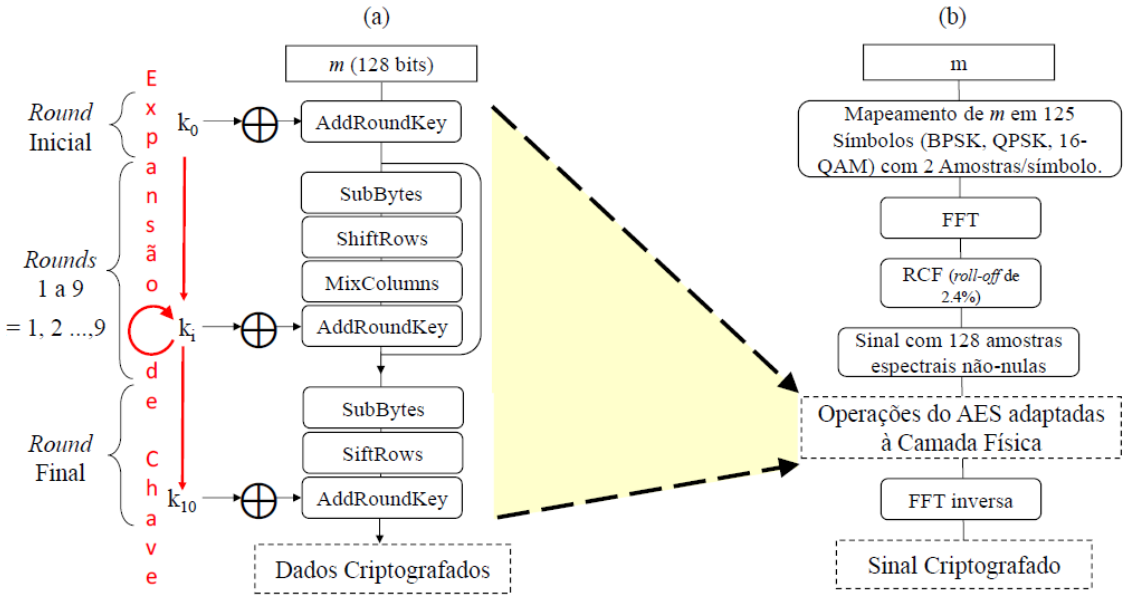

Figura 6

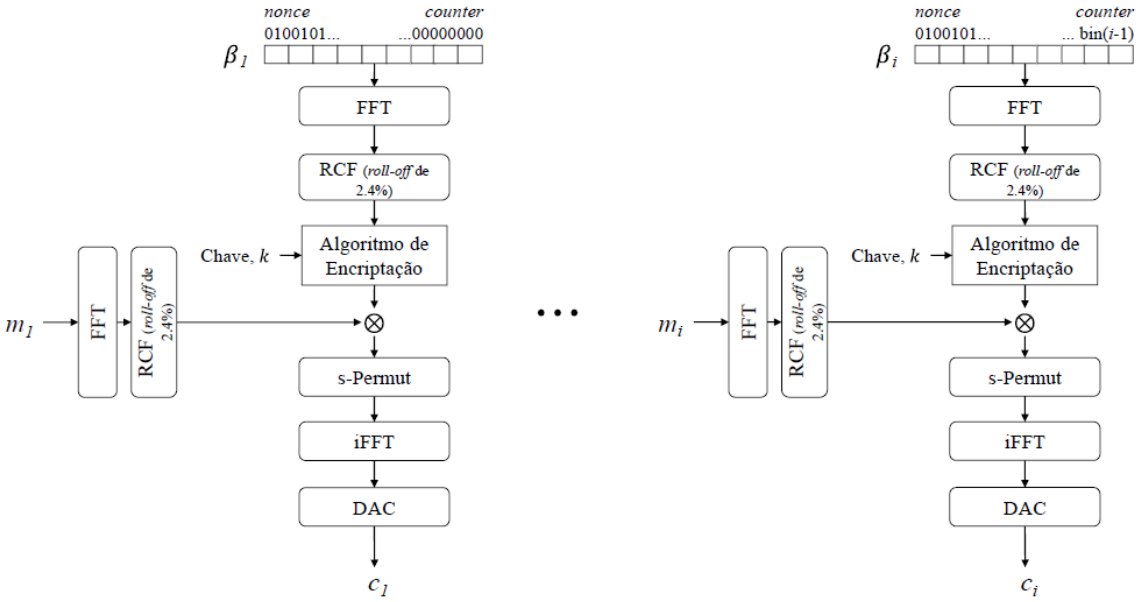

Figura 7

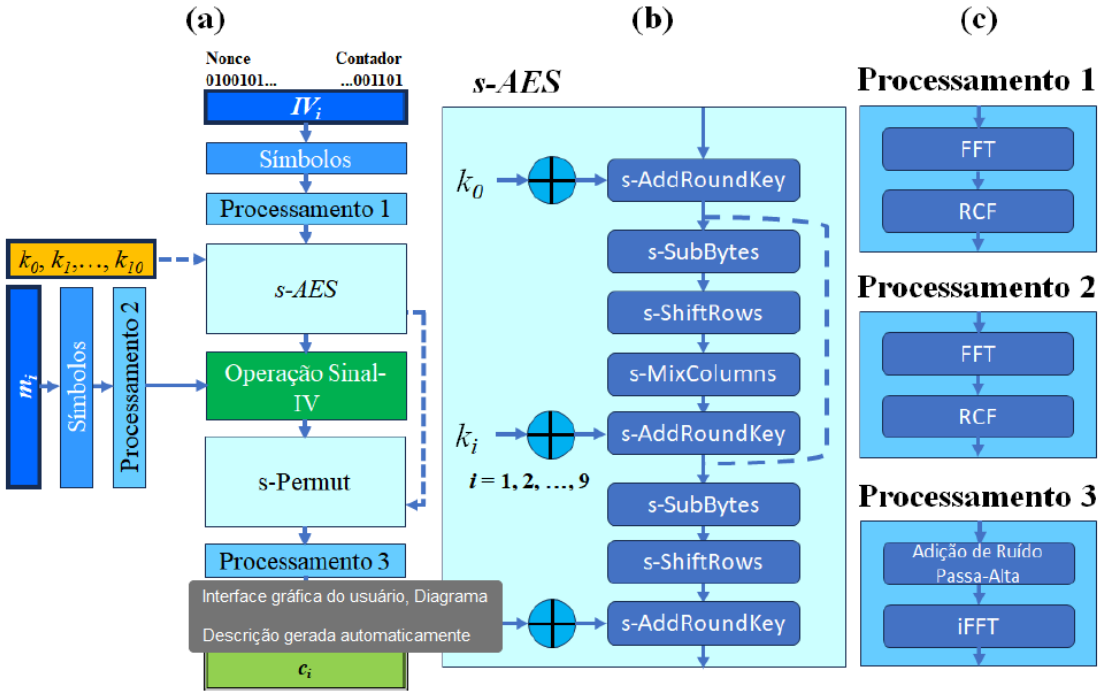

Figura 8

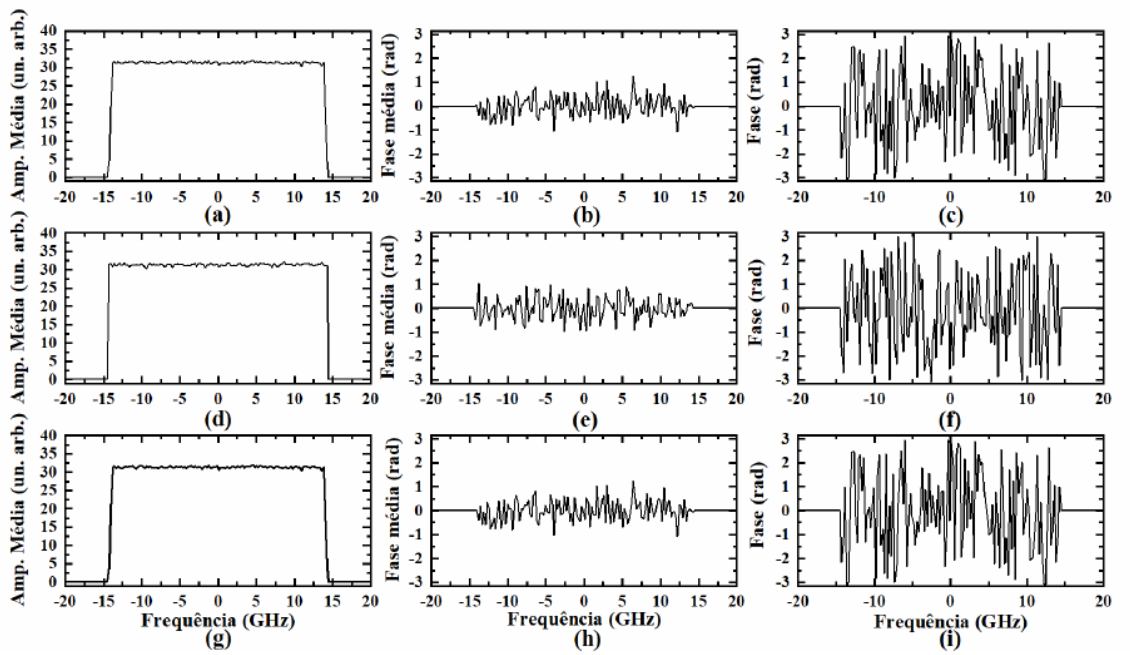

Figura 9

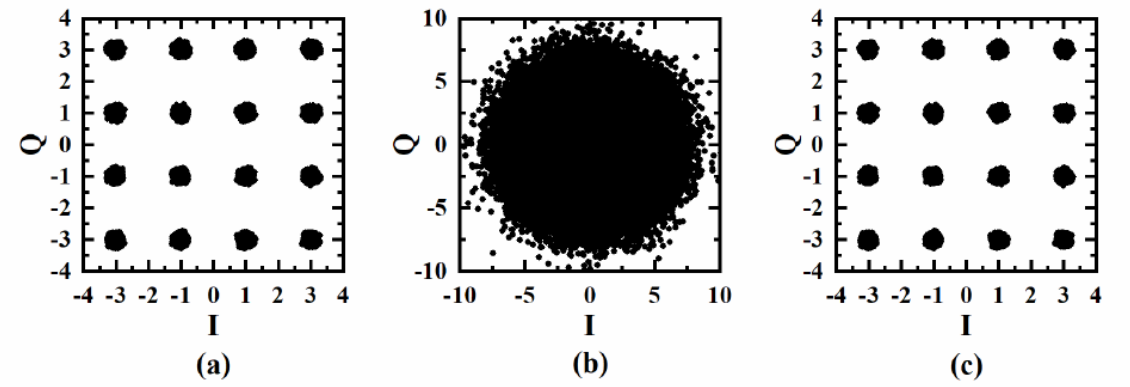

Figura 10

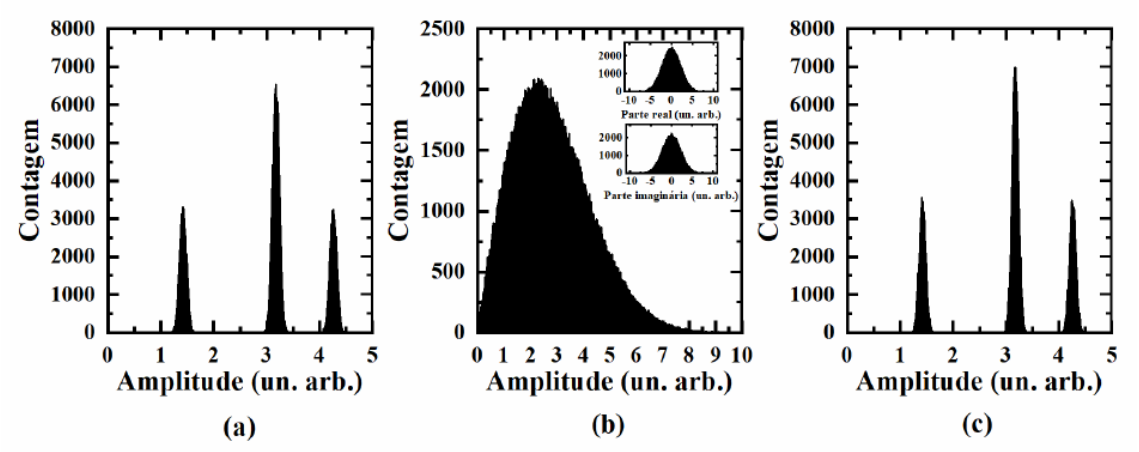

Figura 11

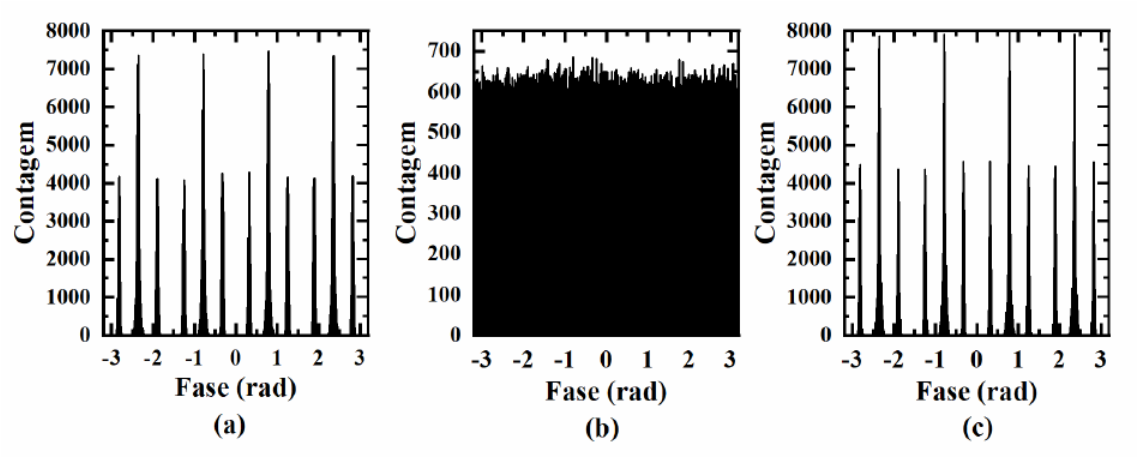

Figura 12

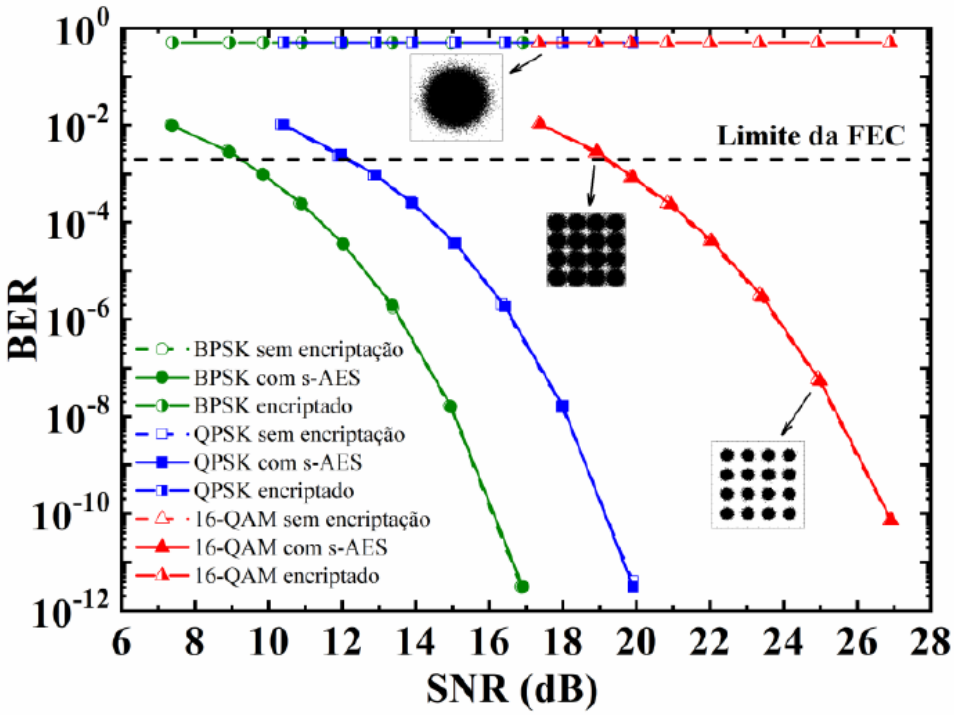
BER
SNR (dB)
Limite da FEC
BPSK sem encriptação
BPSK com s-AES
BPSK encriptado
QPSK sem encriptação
QPSK com s-AES
QPSK encriptado
16-QAM sem encriptação
16-QAM com s-AES
16-QAM encriptado

Figura 13

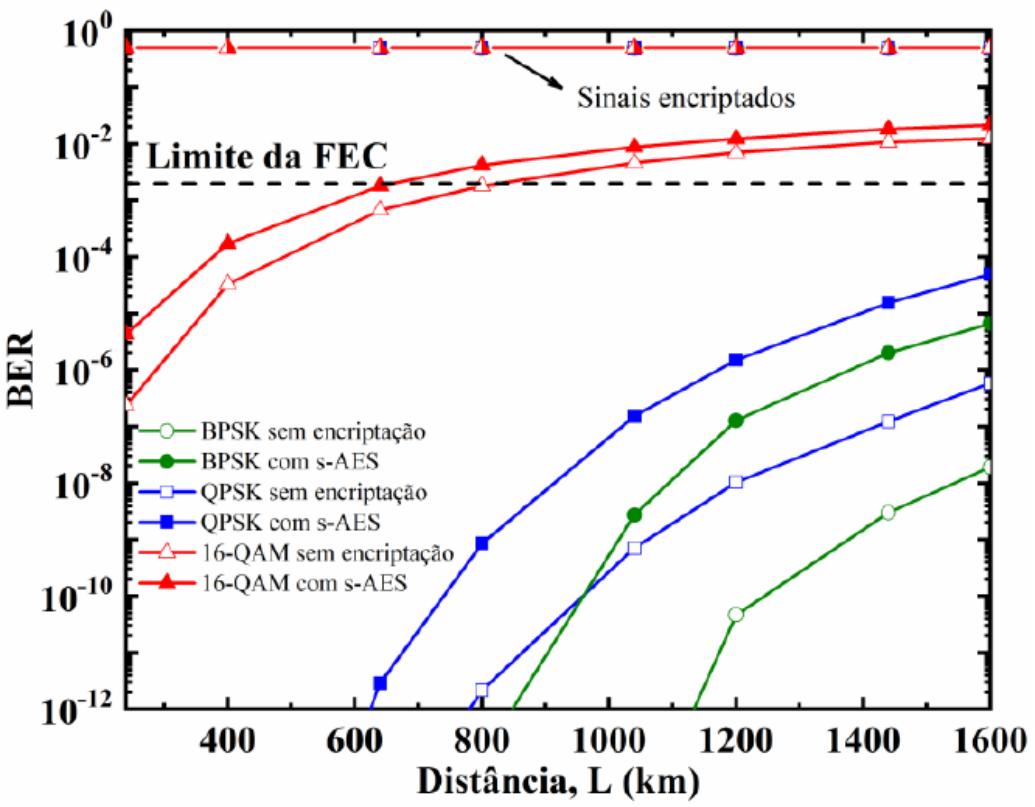
Sinais encriptados
Limite da FEC
BER
Distância, L (km)
BPSK sem encriptação
BPSK com s-AES
QPSK sem encriptação
QPSK com s-AES
16-QAM sem encriptação
16-QAM com s-AES

Figura 14

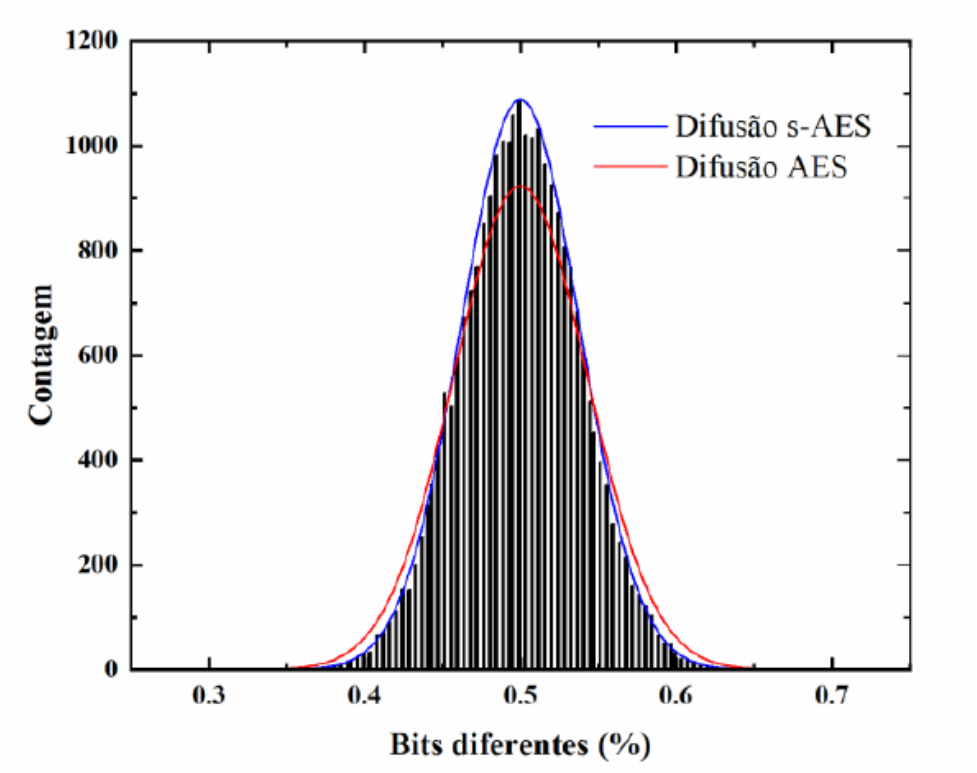
1200
1000
800
600
400
200
0
Contagem
0.3
0.4
0.5
0.6
0.7
Bits diferentes (%)
Difusão s-AES
Difusão AES

Figura 15

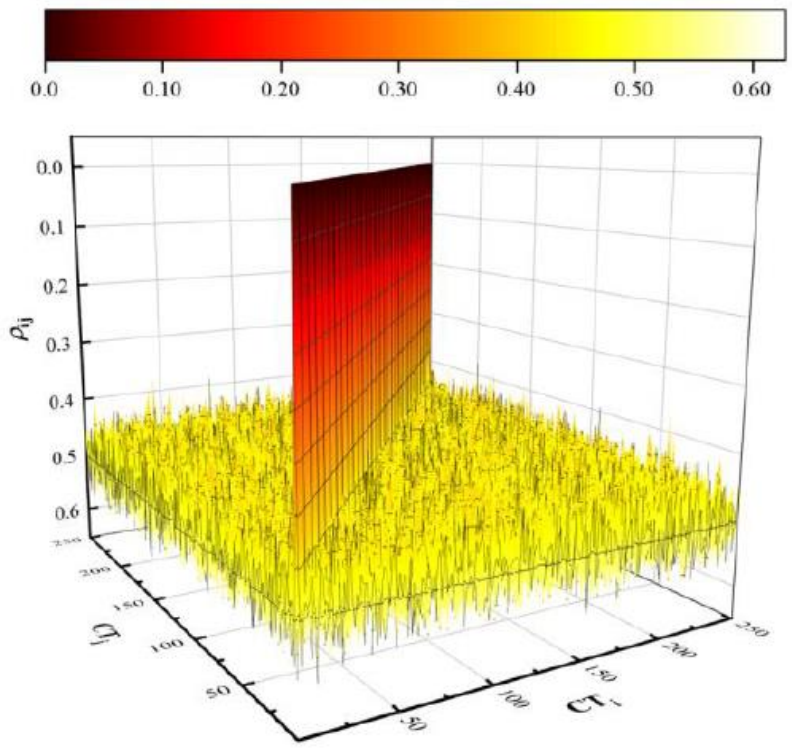
0.0
0.10
0.20
0.30
0.40
0.50
0.60
ρ_{ij}
0.0
0.1
0.2
0.3
0.4
0.5
0.6
250
200
150
100
50
i,j
-250
-200
-150
-100
-50
E_F

Figura 16

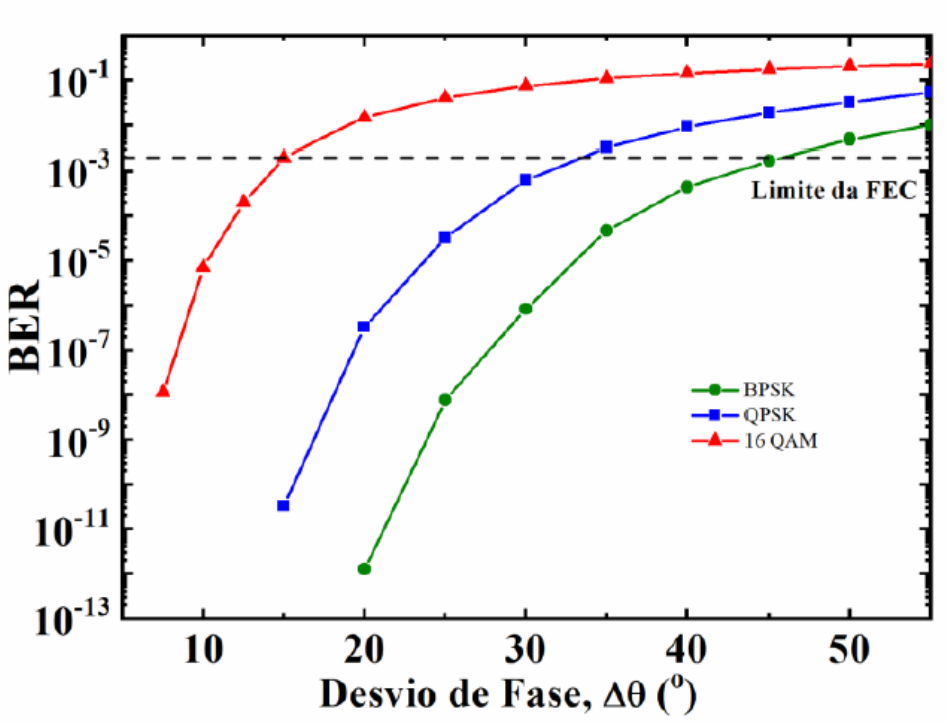

Figura 17

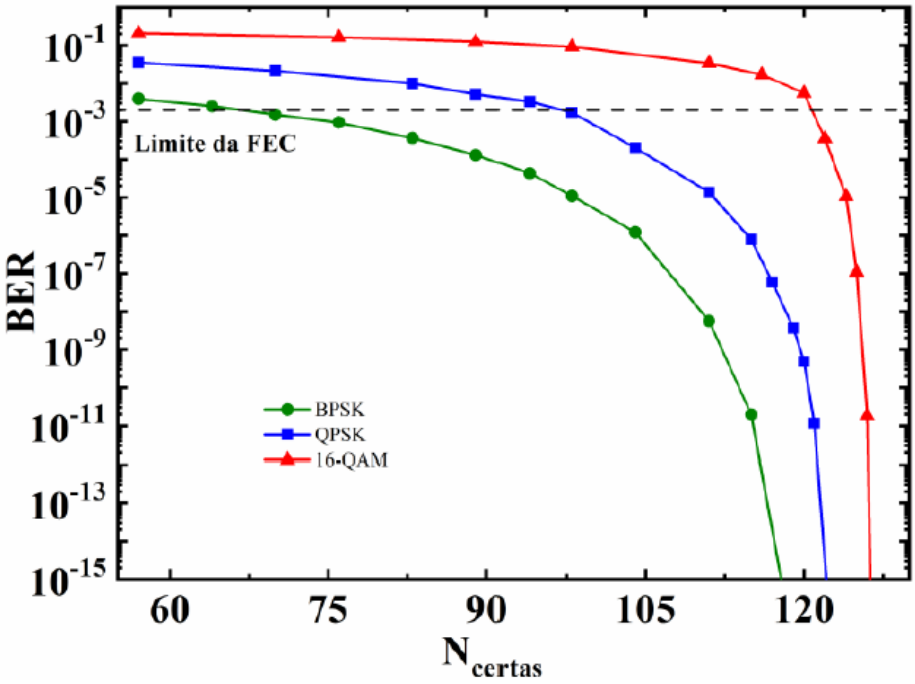

Figura 18

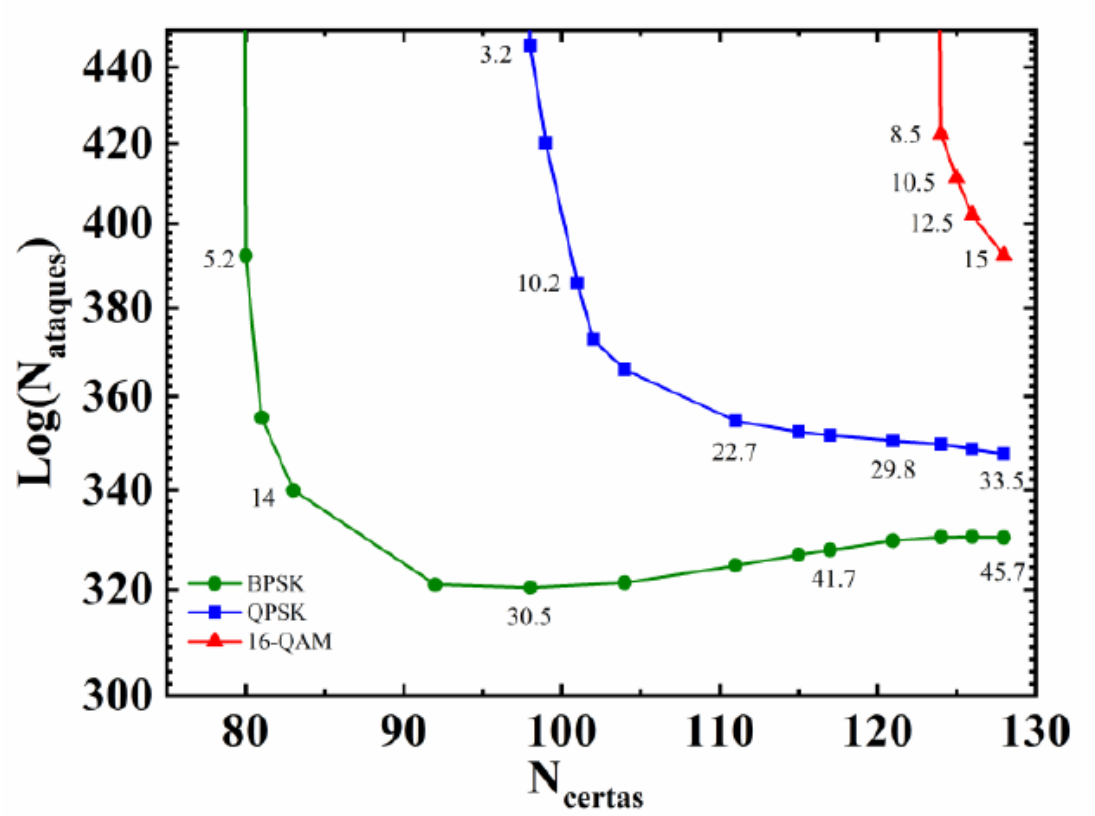
Log(N ataques)
N certas
BPSK
QPSK
16-QAM
5.2
14
30.5
41.7
45.7
3.2
10.2
22.7
29.8
33.5
8.5
10.5
12.5
15

Figura 19

RESUMO

MÉTODO PARA ENCRIPTAR OS SINAIS REFERENTES A VÁRIOS BLOCOS COM UMA ÚNICA CHAVE CRIPTOGRÁFICA

Trata a presente invenção de um novo método que atua no sentido de criptografar sinais discretos da chamada Subcamada Dependente do Meio na Camada Física de um sistema de comunicações, que é a camada responsável por converter a informação digital em sinais, o qual a partir de uma estratégia inédita em que as chaves criptográficas podem ser reutilizadas. O método proposto é referente à criptografia de sinais discretos. Esse método é o único conhecido que permite a reutilização da mesma chave criptográfica para encriptar blocos distintos. A reutilização da chave para encriptar diferentes blocos, que é amplamente utilizada em criptografia de dados, permite a encriptação paralela de vários blocos de sinais tornando o processo mais rápido e seguro, incorporando à criptografia de sinais e operações que são seguras e amplamente utilizadas na criptografia de dados.