UNIVERSIDADE ESTADUAL PAULISTA JÚLIO DE MESQUITA FILHO
CÂMPUS DE SÃO JOÃO DA BOA VISTA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

WELERSON SANTOS SOUZA

Adaptação de Criptografia Espectral ao Paradigma do *Advanced Encryption Standard*

São João da Boa Vista
2021

WELERSON SANTOS SOUZA

Adaptação de Criptografia Espectral ao Paradigma do *Advanced Encryption Standard*

Versão original

Dissertação apresentada à Universidade Estadual Paulista Júlio de Mesquita Filho - Câmpus de São João da Boa Vista para obtenção do título de Mestre em Engenharia Elétrica pelo Programa de Pós-graduação em Engenharia Elétrica.

Área de concentração: Automação e Sistemas Eletrônicos

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

Coorientador: Prof. Dr. Ivan Aritz Aldaya Garde

São João da Boa Vista

2021

S729a

Souza, Welerson Santos
Adaptação de criptografia espectral ao paradigma do "Advanced Encryption Standard" / Welerson Santos Souza. -- São João da Boa Vista, 2021
95 f. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Câmpus Experimental de São João da Boa Vista, São João da Boa Vista
Orientador: Marcelo Luís Francisco Abbade

1. Criptografia. 2. Segurança de sistemas. 3. Comunicações ópticas. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Câmpus Experimental de São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus Experimental de São João da Boa Vista

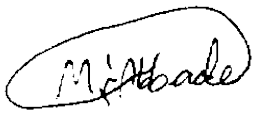
CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Adaptação de Criptografia Espectral ao Paradigma do "Advanced Encryption Standard"

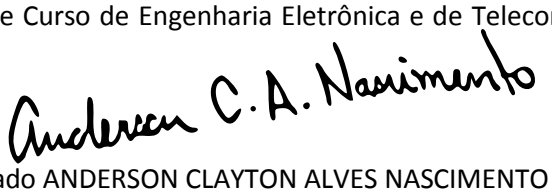
AUTOR: WELERSON SANTOS SOUZA

ORIENTADOR: MARCELO LUÍS FRANCISCO ABBADE

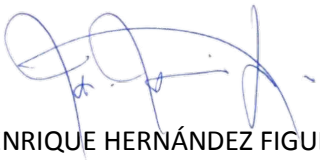
Aprovado como parte das exigências para obtenção do Título de Mestre em ENGENHARIA ELÉTRICA, área: Sistemas Eletrônicos pela Comissão Examinadora:



Prof. Dr. MARCELO LUÍS FRANCISCO ABBADE (Participaçao Virtual)
Coordenadoria de Curso de Engenharia Eletrônica e de Telecomunicações / Câmpus de São João da Boa Vista



Professor Associado ANDERSON CLAYTON ALVES NASCIMENTO (Participaçao Virtual)
Institute of Technology / University of Washington



Professor Titular HUGO ENRIQUE HERNÁNDEZ FIGUEROA (Participaçao Virtual)
Departamento de Comunicações / Unicamp - Faculdade de Engenharia Elétrica e de Comunicações

Prof. Dr. MURILO ARAÚJO ROMERO (Participação Virtual)
Departamento de Engenharia Elétrica e Computação / EESC/ Universidade de São Paulo

São João da Boa Vista, 12 de Fevereiro de 2021

Dedico esse trabalho à minha irmã Giovanna, que desperta a melhor parte de mim, está sempre ao meu lado e me apoia incondicionalmente.

Agradecimentos

Agradeço aos meus pais, Dacia e Emerson, por todo suporte e apoio durante toda minha vida. Por comemorarem minhas vitórias como se fossem deles e me motivarem em seguir os meus sonhos.

À minha irmã Giovanna, por ser minha companheira de todas as horas e lutar comigo todas as batalhas da vida.

Aos professores Marcelo Luís Francisco Abbade e Ivan Aritz Aldaya Garde, respectivamente orientador e coorientador desse trabalho, por todo ensinamento que me proporcionaram, pelo apoio técnico e pela amizade que construímos no desenvolvimento do trabalho.

À Universidade Virtual do Estado de São Paulo, pela bolsa de mestrado concedida entre os meses de fevereiro de 2019 e fevereiro de 2020.

À Fundação de Amparo a Pesquisa do Estado de São Paulo (FAPESP) pelo financiamento, em caráter de bolsa de mestrado, sob o processo nº 2019/14858-3, Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), entre 01/03/2020 e 31/01/2021.

Aos meus amigos, por compartilharem comigo tantos bons momentos, me apoiarem nas minhas decisões, confiarem em mim e me fazerem ver o lado bom da vida sempre que as coisas ficam difíceis.

Por fim, agradeço a todos que me fizeram crescer como pessoa e profissional durante a realização desse trabalho.

"Nós só podemos ver um pouco do futuro, mas o suficiente para perceber que há muito a fazer."

(Alan Mathison Turing)

Resumo

SOUZA, Welerson Santos. **Adaptação de Criptografia Espectral ao Paradigma do *Advanced Encryption Standard***. 2021. 95 f. Dissertação (Mestrado em Engenharia Elétrica) – Câmpus Experimental de São João da Boa Vista, Universidade Estadual Paulista Júlio de Mesquita Filho, São João da Boa Vista, 2021.

Confidencialidade é um dos pilares de segurança da informação e está relacionada à privacidade de informações transmitidas entre pessoas ou dispositivos. Técnicas de criptografia processam as informações antes de serem transmitidas para dificultar que interceptadores compreendam seu conteúdo original. Em sistemas de comunicações modernos, técnicas de criptografia de dados processam bits para prover confidencialidade nas camadas superiores do modelo *Open System for Interconnections* (OSI), ou seja, entre as camadas de Enlace e de Aplicação. A criptografia de dados está bem estabelecida e conta com diversos padrões comerciais. Um dos padrões mais seguros e mais utilizados atualmente é o *Advanced Encryption Standard* (AES), que conta com redes de substituição e permutação para prover as propriedades de difusão e confusão estabelecidas por Shannon às mensagens cifradas e é semanticamente seguro. Além disso, os modos de operação, definidos em criptografia de dados, tornam aleatórias as mensagens cifradas e possibilitam a reutilização de chaves. Entre esses modos destaca-se o *Counter Mode* (CTR mode), em que a técnica de criptografia utilizada atua sobre um vetor de inicialização. O CTR pode ser paralelizado, ou seja, diversos processadores podem encriptar vários blocos simultaneamente. A camada Física do modelo OSI faz a conversão de bits para sinais em que técnicas de criptografia de sinais podem ser utilizadas. Embora a criptografia de sinais não conte com padrões comerciais, é um tópico de pesquisa emergente e tem apresentado bons resultados de segurança. O objetivo desse trabalho é desenvolver e avaliar uma nova técnica de criptografia espectral de sinais. A nova técnica é uma adaptação do padrão de criptografia AES e do modo de operação CTR para a camada física, essa técnica é denominada s-AES/s-CTR, em que o "s-"é utilizado para indicar que as técnicas foram definidas para o domínio de sinais. Foram estabelecidas analogias entre os algoritmos definidos em criptografia de dados e os algoritmos propostos nesse trabalho para que as operações do AES e do CTR fossem adaptadas para o domínio de sinais. Os resultados das análises realizadas sugerem que o s-AES/s-CTR encripta e desencripta os sinais de maneira satisfatória. Em particular, sinais criptografados podem ser transmitidos sem penalidades por canais AWGN (*Additive white Gaussian noise*) e podem ser propagados por canais ópticos de até 650 km. Com relação a segurança, o s-AES/s-CTR provê as propriedades de difusão e confusão aos sinais criptografados. A segurança da técnica contra ataques de força bruta também foi avaliada e mostra que um interceptador deve fazer, no mínimo, 10^{320} ataques para garantir que conseguirá recuperar o sinal corretamente. A utilização do modo de operação, além de tornar a técnica robusta contra ataques de texto escolhido, viabiliza a reutilização de chaves. No melhor de nosso conhecimento, é a primeira vez que uma técnica de criptografia de sinais possibilita a reutilização de chaves criptográficas.

Palavras-chaves: Segurança de Redes. Processamento Digital de Sinais. Redes Ópticas. Criptografia de Sinais.

Abstract

SOUZA, Welerson Santos. **Adaptation of Spectral Encryption to the Advanced Encryption Standard Paradigm.** 2021. 95 p. Dissertation (Master of Electrical Engineering) – Campus São João da Boa Vista, São Paulo State University, São João da Boa Vista, 2021.

Confidentiality is one of the pillars of information security and is related to the privacy of information transmitted between people or devices. Encryption techniques process information before it is transmitted to make it difficult for eavesdropper to understand its original content. In modern communications systems, data encryption techniques process bits to provide confidentiality in the upper layers of the Open System for Interconnections (OSI) model, that is, between the Link and Application layers. Data encryption is well established and has several commercial standards. One of the safest and most widely used standards today is Advanced Encryption Standard (AES), which has substitution and permutation networks to provide the diffusion and confusion properties established by Shannon to encrypted messages and is semantically secure. In addition, the modes of operation, defined in data encryption, randomize encrypted messages and make it possible to reuse keys. Among these modes, Counter Mode (CTR mode) stands out, in which the encryption technique used acts on an initialization vector. The CTR mode can be parallelized, that is, several processors can encrypt several blocks simultaneously. Physical layer of the OSI model converts bits to signals in which signal encryption techniques can be used. Although signal encryption does not have commercial standards, it is an emerging research topic and has shown good security results. The objective of this work is to develop and evaluate a new technique of spectral signal cryptography. The new technique is an adaptation of the AES and the CTR mode of operation for the physical layer, this technique is called s-AES/s-CTR, in which the "s-"is used to indicate that the techniques were defined for the signal domain. The results of the analyzes suggest that the s-AES / s-CTR encrypts and decrypts the signals satisfactorily. In particular, encrypted signals can be transmitted without penalty through AWGN (Additive white Gaussian noise) channels and can be propagated through optical channels up to 650 km. Regarding security, the s-AES/s-CTR provides the diffusion and confusion properties for encrypted signals. The safety of the technique against brute force attacks has also been verified and shows that an interceptor must make at least 10^{320} attacks to ensure that it will be able to recover the signal correctly. The mode of operation, in addition to making the technique robust against attacks of chosen text, make it possible to reuse the keys. To the best of our knowledge, this is the first time that a signal encryption technique has enabled the reuse of cryptographic keys.

Keywords: Network Security. Digital Signal Processing. Optical Networks. Signal Encryption.

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

AES	*Advanced Encryption Standard* (Padrão de Criptografia Avançado)
ASE	*Amplified spontaneous emission* (Emissão espontânea amplificada)
AUIN	Agência Unesp de Inovação
AWGN	*Additive white Gaussian noise* (Ruído aditivo Gaussiano e branco)
BER	*Bit error rate* (Taxa de erro de bit)
BFA	*Brute-force attack* (Ataque por força bruta)
BPSK	*Binary Phase Shift Keying* (Modulação por deslocamento de fase binária)
CBC	*Cipher Block Chaining* (Cifra de blocos encadeados)
CTR	*Counter Mode*
DAC	*Digital-to-analog converter* (Conversor digital-analógico)
dB	Decibel
DCF	*Dispersion-compesating fiber*(Fibra compensadora de dispersão)
DES	*Data Encryption Standard* (Padrão de criptografia de dados)
DSP	*Digital signal processing* (Processamento digital de sinais)
EDFA	*Erbium-doped fiber amplifier* (Amplificador de fibra dopada com érbio)
FEC	*Forward error correction* (Correção de erros a frente)
FFT	*Fast Fourier transform* (Transformada rápida de Fourier)
FPGA	*Field Programmable Gate Array* (Arranjo de portas programáveis em campo)
Gbps	Giga bits por segundo
GHz	Gigahertz

I	*In-phase* (Componente em fase do sinal)
iFFT	*Inverse fast Fourier transform* (transformada rápida inversa de Fourier)
IV	*Initialization Vector* (Vetor de inicialização)
km	Kilometro
nm	Nanometro
OFB	*Output Feedback Mode* (Modo de feedback de saída)
OFDM	*Orthogonal frequency domain multiplexing* (Multiplexação por divisão em frequências ortogonais)
OSI	*Open System for Interconnections* (Interconexão de sistemas abertos)
PLE	*Physical layer encryption* (Criptografia na camada física)
PPA	*Probabilistic polynomial-time algorithm* (Algoritmo probabilístico em tempo polinomial)
PRBS	*Pseudorandom binary sequence* (Sequência binária pseudo-aleatória)
ps	Picosegundo
PSGs	*Pseudo-random generators* (Geradores pseudo aleatórios)
P/S	Conversor paralelo-série
Q	*Quadrature* (Componente em quadratura do sinal)
QAM	*Quadrature Amplitude Modulation* (Modulação de amplitude em quadratura)
QKD	*Quantum key distribution* (Distribuição quântica de chaves)
QPSK	*Quadrature Phase Shift Keying* (Modulação por deslocamento de fase em quadratura)
RCF	*Raised-cosine filter* (Filtro cosseno-levantado)
RC5	*Rivest Cipher 5*

s-AES	*Advanced Encryption Standard adapted for signals* (Padrão de Criptografia Avançado adaptado para sinais)
s-CTR	*Counter Mode adapted to signals* (Modo CTR adaptado para sinais)
SNR	*signal-to-noise ratio* (Razão sinal-ruído)
SPDE	*Spectral phase and delay encoding* (Codificação espectral por fase e atraso)
SPE	*Spectral phase encoding* (Codificação espectral por fase)
SPN	*Substitution-permutation network* (Rede de substituição e permutação)
SSMF	*Standard single-mode optical fiber* (Fibra óptica monomodo padrão)
s-Box	*Substitution box* (Tabela de substituição)
S/P	Conversor série-paralelo
TEA	*Tiny Encryption Algorithm*
W	Watt
XOR	*Exclusive or* (Ou-exclusivo)

Lista de símbolos

c	Mensagem cifrada
E	Algoritmo de encriptação
k_e	Chave de encriptação
D	Algoritmo de desencriptação
k_d	Chave de desencriptação
L_i	Bits da esquerda de um bloco das redes de Feistel
R_i	Bits da direita de um bloco das redes de Feistel
k_i	Chave do i-ésimo *round* em um algoritmo de encriptação em blocos.
F_c	Função criptográfica
n	Número total de redes de Feistel utilizadas em determinado algoritmo.
n_b	Comprimento, em bits, de um bloco do AES
p^n	Ordem de um Corpo de Galois.
g	Polinômio binário irredutível de grau 8
e_1	Elemento binário 1
e_2	Elemento binário 2
$y(x)$	Elemento binário resultante da multiplicação entre $e1$ e $e2$ no Corpo de Galois
b'	Byte após a operação SubBytes
A	Matriz afim da operação SubBytes
b	Byte antes da operação SubBytes
c_a	Constante afim
s	Matriz 4x4 bytes antes da operação ShiftRows

s'	Matriz 4x4 bytes após a operação ShiftRows
$s_{r,c}$	Byte da r-ésima linha e c-ésima coluna da matriz 4x4 bytes
w	Coluna de entrada da operação MixColumns
w'	Coluna de saída da operação MixColumns
w_i	i-ésimo byte da coluna de entrada da operação MixColumns
w'_i	i-ésimo byte da coluna de saída da operação MixColumns
β_i	Vetor de inicialização do modo CTR
γ_i	Vetor β_i encriptado
$\dot{x}$	Sequência caótica diferencial no eixo x
$\dot{y}$	Sequência caótica diferencial no eixo y
$\dot{z}$	Sequência caótica diferencial no eixo z
$\dot{u}$	Sequência caótica diferencial no eixo u
x	Sequência caótica no eixo x
y	Sequência caótica no eixo y
z	Sequência caótica no eixo z
u	Sequência caótica no eixo u
t_i	Constante utilizada em um sistema caótico
N_{sub}	Número de subportadoras OFDM
N_{simb}	Número de símbolos OFDM
p	Posição inicial de símbolos OFDM
P'	Posição final de símbolos OFDM
ΔI	Parâmetro caótico de deslocamento em I
ΔQ	Parâmetro caótico de deslocamento em Q

n_s	Número de fatias em uma técnica de criptografia por fatiamento espectral
f_c	Frequência da portadora
N_a	Número de ataques
$\Delta\theta$	Desvio de fase
$e_I(t)$	Sinal em fase encriptado
$e_Q(t)$	Sinal em quadratura encriptado
$e(t)$	Sinal encriptado
F	Função mapeamento de fases
φ_{in}	Fase de entrada da função F
θ_{out}(j)	Fase da j-ésima amostra do sinal de saída da operação AddRoundKey
θ_{in}(j)	Fase da j-ésima amostra do sinal de entrada da operação AddRoundKey
θ(i,j)	j-ésima fase da s-chave k_{i}
B	Banda do sinal
s[k]	Sinal original amostrado
e[k]	Sinal encriptado amostrado
n[k]	Ruído amostrado
z[k]	Sinal desencriptado ruídoso
θ_i	Fase da i-ésima amostra do sinal original
χ_i	Fase da i-ésima amostra do vetor γ_i
$N_{ataques,f}$	Número de FBAs em um ataque nas fases do sinal
N_{certas}	Número de amostras na posição correta
$N_{ataques,p}$	Número de FBAs em um ataque nas posições das amostras

Sumário

[1] De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

1 Introdução

Nesse capítulo, iremos abordar aspectos históricos e realizaremos uma breve revisão a respeito de tópicos relevantes inerentes à criptografia de dados e de sinais. Além disso, apresentaremos as principais contribuições do nosso trabalho e explicitaremos a organização do restante da dissertação. A Seção 1.1 é reservada aos fundamentos da criptografia de dados e de sinais. As Seções 1.2 e 1.3 apresentam, respectivamente, as contribuições e a organização do trabalho.

1.1 Fundamentos da criptografia

A segurança da informação apoia-se em três pilares para proteger sistemas de comunicação: confidencialidade, integridade e disponibilidade (SCARFONE; JANSEN; TRACY, 2008). Confidencialidade está relacionada à privacidade das informações, ou seja, apenas pessoas ou dispositivos autorizados devem ser capazes de compreender corretamente as informações. Integridade visa garantir que a informação não sofra nenhuma alteração entre o transmissor e o receptor. Além disso, a informação não deve chegar em um receptor que não tenha sido escolhido pelo transmissor. Por fim, disponibilidade é o pilar da segurança que diz respeito à acessibilidade das informações. Pessoas ou dispositivos autorizados devem ter acesso a elas sempre que necessário.

A criptografia, do grego "kryptós" (escondido) e "graphéin" (escrita), consiste de técnicas utilizadas para dificultar que interceptadores compreendam o conteúdo de informações trocadas entre pessoas ou dispositivos. As técnicas de criptografia estão inseridas nos pilares de confidencialidade e de integridade da segurança da informação. Além de serem amplamente utilizadas para conferir segurança à transmissão de informações entre um transmissor e um receptor, técnicas de criptografia são fundamentais no processo de autenticidade de uma comunicação. Em autenticação, técnicas de criptografia são utilizadas para garantir que a identidade alegada pelas partes envolvidas na comunicação seja verdadeira.

No contexto de confidencialidade, civilizações antigas já utilizavam alguns métodos simples para criptografar mensagens. O bastão de Licurgo (Scytale Espartano), por exemplo, foi utilizado em Esparta para conferir segurança às comunicações militares (KELLY, 1998).

O Scytale Espartano consistia em um bastão de madeira em que o remetente enrolava uma tira e escrevia uma mensagem verticalmente. Após escrever, o emitente retirava a tira do bastão e enviava ao destinatário por meio de um mensageiro, que usava a tira como um cinto com as letras viradas para o corpo. O destinatário, ao receber a mensagem, enrolava a tira em um bastão com o mesmo diâmetro do bastão utilizado pelo remetente. Caso o destinatário não utilize um bastão com as mesmas características físicas do bastão utilizado pelo transmissor, a mensagem não é interpretada corretamente.

Outro exemplo importante na criptografia clássica é a Máquina Enigma. Criada em 1918, foi um dispositivo amplamente adotado pelo exército e pela marinha da Alemanha durante a Segunda Guerra Mundial (SMART, 2016). A Máquina Enigma encripta mensagens realizando a substituição de letras. Quando uma letra é pressionada, a máquina realiza um processo com rotores em que outra letra é gerada e compõe a mensagem cifrada. Entretanto, esse dispositivo tinha uma deficiência. A letra que compõe a mensagem cifrada nunca é igual à letra pressionada. Essa foi uma das características importantes para que a segurança da Máquina Enigma fosse quebrada.

Até a Máquina Enigma, as técnicas de criptografia eram baseadas em letras. Com a invenção do computador, as técnicas de criptografia passaram a realizar operações em bits e não em letras. Com o passar dos anos, o avanço computacional possibilitou que inúmeras técnicas de criptografia fossem desenvolvidas para garantir segurança da informação. A criptografia moderna é baseada no trabalho seminal de Shannon (SHANNON, 1949) e atualmente, grande parte dos sistemas de comunicações utilizam técnicas de criptografia para prover segurança contra invasores.

No contexto dos sistemas de comunicações modernos, o modelo de referência para Interconexão de Sistemas Abertos (*Open System for Interconnections*, OSI) conta com 7 camadas para padronizar a comunicação de redes: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física (TANENBAUM; WETHERALL, 2010). Técnicas de criptografia de dados processam conjuntos de bits para prover segurança nas seis camadas superiores do modelo OSI, ou seja, entre as camadas de Enlace e de Aplicação.

A criptografia de dados está bem estabelecida e conta com diversos padrões comerciais seguros. Muitos desses padrões utilizam uma estrutura de criptografia chamada Redes de Feistel (MENEZES *et al.*, 1996). Nessa estrutura, a mensagem é dividida em dois blocos que são submetidos periodicamente à operações criptográficas. Um padrão importante que utiliza as redes de Feistel é o padrão DES (*Data Encryption Standard*)

(PUB, 1977), que conta com 16 rodadas de Redes de Feistel para criptografar os sinais, além de outras operações que serão descritas posteriormente. O padrão de criptografia de dados mais utilizado atualmente é o AES (*Advanced Encryption Standard*) (RIJMEN; DAEMEN, 2001; FIPS, 2001). O AES realiza consecutivas operações de ou exclusivo (*exclusive or*, XOR), substituição e permutação para conferir segurança às mensagens cifradas. A descrição detalhada desses algoritmos de encriptação é encontrada no Capítulo 2.

É de extrema importância que algoritmos de criptografia sejam seguros contra ataques de invasores. Shannon observou (SHANNON, 1949) que algoritmos de criptografia devem conferir as propriedades de difusão e confusão às mensagens cifradas para serem seguros. A propriedade de difusão estabelece que a influência de um bit da mensagem original deve ser espalhada em vários bits da mensagem cifrada. Enquanto isso, a propriedade de confusão relaciona o algoritmo de criptografia com a chave criptográfica. A chave deve ser complexa de modo que a influência de cada bit da chave seja espalhada em vários bits da mensagem cifrada. O padrão de criptografia de dados AES é seguro e atende as propriedades de confusão e difusão estabelecidas por Shannon.

Outra definição importante no contexto de segurança das técnicas de criptografia é a segurança semântica. Uma técnica é considerada semanticamente segura se não há nenhum algoritmo probabilístico em tempo polinomial (*Probabilistic polynomial-time algorithm*, PPA) que possa determinar qualquer informação da mensagem original por meio da mensagem cifrada (SHAFI; SILVIO, 1982). Por exemplo, cifras que utilizam geradores pseudo-aleatórios (*pseudo-random generators*, PSGs) para gerar as chaves criptográficas são semanticamente seguras (KATZ; LINDELL, 2014).

Grande parte dos algoritmos de criptografia de dados é determinístico, portanto, não conferem segurança semântica às mensagens cifradas. Para que determinada técnica criptografia de dados seja probabilística, modos de operação são associados aos algoritmos de encriptação. Os modos de operação são construídos de maneira que as mensagens cifradas sejam aleatórias.

A camada física converte os bits provenientes das camadas superiores em sinais que serão propagados pelos meios físicos de transmissão. Como a criptografia de dados opera bits, não é possível aplicar técnicas de criptografia de dados nesses sinais que serão propagados. Para que os sinais provenientes da camada física sejam criptografados, a criptografia de sinais vem sendo estudada e embora ainda não tenha nenhum padrão

comercial, é um tópico promissor de pesquisa e pode complementar à criptografia de dados para aumentar a segurança total do sistema de comunicação.

Quando uma técnica de criptografia de dados é utilizada em determinada camada do modelo OSI, os dados do *payload* da camada imediatamente superior são encriptados, mas o cabeçalho inserido pela camada que realiza a criptografia não. Quando a criptografia é realizada na camada mais inferior do modelo OSI, garante-se que todos os *payloads* e cabeçalhos sejam protegidos (FOK *et al.*, 2011). Dessa forma, a informação de todas as camadas superiores do modelo OSI é protegida. De fato, a criptografia de sinais pode ser complementar à criptografia de dados. Em redes de comunicação, os sinais podem trafegar por meios que não pertencem ao proprietário das informações transmitidas. Olhando por esse ponto de vista, também é interessante que o sinal seja criptografado para que o proprietário desse meio não consiga interpretar as informações corretamente.

A criptografia de sinais pode ser dividida entre criptografia de sinais em banda passante (BENNETT; BRASSARD, 1984; EKERT, 1991; BENNETT; BRASSARD; EKERT, 1992; BENNETT *et al.*, 1992; YIN *et al.*, 2016; MAO *et al.*, 2018; LIAO *et al.*, 2017; KE *et al.*, 2016; HOU *et al.*, 2016; YI *et al.*, 2018; CORNEJO; PEREZ *et al.*, 2007; ABBADE *et al.*, 2014; ABBADE *et al.*, 2015; ABBADE *et al.*, 2017; ABBADE *et al.*, 2018; SANTOS *et al.*, 2019) e criptografia de sinais em banda base (ODEN *et al.*, 2017; GENG *et al.*, 2018; HU *et al.*, 2015; YANG *et al.*, 2016; SULTAN *et al.*, 2018; ABBADE *et al.*, 2018; ABBADE *et al.*, 2019; SOUZA *et al.*, 2020; SANTOS, 2020). Dentre as técnicas de criptografia de sinais encontradas na literatura, serão apresentadas nesse trabalho as técnicas de criptografia baseadas em comunicação quântica que criptrografam sinais em banda passante, as técnicas de criptografia caótica que criptografam sinais em banda base e as técnicas de criptografia por fatiamento espectral, que criptografam sinais em banda passante e em banda base.

A comunicação quântica utiliza uma única partícula quântica para representar uma unidade de informação e permite que o transmissor e o receptor monitorem os sinais transmitidos e notem a presença de interceptadores. A partícula quântica pode ser, por exemplo, o elétron (partícula quântica elétrica) ou o fóton (partícula quântica de luz). Nesse trabalho, denominaremos a criptografia baseada em comunicação quântica como criptografia quântica. Usualmente, a criptografia quântica tem como partícula quântica o fóton (BENNETT; BRASSARD, 1984; EKERT, 1991; BENNETT; BRASSARD; EKERT, 1992; BENNETT *et al.*, 1992). Por ser limitada a taxas de transmissão baixas, a criptografia

quântica tem como maior aplicação a troca de chaves criptográficas entre as estações (YIN *et al.*, 2016; MAO *et al.*, 2018; LIAO *et al.*, 2017).

A criptografia caótica utiliza sistemas caóticos para realizar operações de criptografia de sinais. As técnicas de criptografia caótica podem ser divididas entre técnicas de criptografia caótica e técnicas de criptografia digital caótica. As técnicas de criptografia caótica realizam operações em sinais modulados (KE *et al.*, 2016; HOU *et al.*, 2016; YI *et al.*, 2018) e as técnicas de criptografia digital caótica processam sinais em banda base (ODEN *et al.*, 2017; GENG *et al.*, 2018; HU *et al.*, 2015; YANG *et al.*, 2016; SULTAN *et al.*, 2018).

Por fim, a criptografia por fatiamento espectral divide o sinal no domínio da frequência em fatias espectrais e realiza operações que alteram propriedades físicas do sinal, como por exemplo a amplitude, a fase e a posição das fatias. Estratégias de criptografia por fatiamento espectral em sinais ópticos são encontradas em (CORNEJO; PEREZ *et al.*, 2007; ABBADE *et al.*, 2014; ABBADE *et al.*, 2015; ABBADE *et al.*, 2017; ABBADE *et al.*, 2018; SANTOS *et al.*, 2019). As operações da criptografia por fatiamento espectral podem ser definidas de inúmeras maneiras e aplicadas a sinais em banda base utilizando processamento digital de sinais (*digital signal processing*, DSP) (ABBADE *et al.*, 2018; ABBADE *et al.*, 2019; SOUZA *et al.*, 2020; SANTOS, 2020).

O uso de DSP em técnicas de criptografia de sinais possibilita que uma infinidade de operações criptográficas sejam realizadas com facilidade mantendo a taxa de transmissão e a banda do sinal original. Dessa maneira, justifica-se propor uma nova técnica de criptografia de sinais implementada por meio de DSP. A criptografia de sinais e as principais técnicas citadas anteriormente são abordadas em detalhes no Capítulo 3.

1.2 Objetivos e contribuições do trabalho

O objetivo principal desse trabalho foi desenvolver uma técnica de criptografia de sinais análoga ao AES. Essa técnica é denominada s-AES (*Advanced Encryption Standard adapted for signals*). Para atingir esse objetivo, foi necessário realizar várias propostas que constituem as contribuições desse trabalho, são elas: (1) Adaptação de operações de criptografia de dados para o domínio de sinais; (2) Implementação do s-AES (utilizando as operações desenvolvidas em (1)) em *software*; (3) Avaliação da segurança do s-AES;

(4) Adaptação e implementação de um modo de operação para o domínio de sinais e (5) Obtenção de uma estratégia geral de criptografia que permite a reutilização de uma única chave para encriptar todos os blocos. A seguir, explicaremos as principais características de cada uma das contribuições do trabalho.

(1) Operações de criptografia utilizadas pelas técnicas modernas de criptografia de dados são projetadas para atender determinados requisitos de segurança definidos em criptografia de dados. Estabelecer operações análogas à essas para o domínio de sinais é um caminho importante no sentido da criação de técnicas seguras de criptografia de sinais.

(2) O s-AES está implementado em um *software* escrito em MATLAB. O *software* é habilitado para criptografar sinais em banda base. Destaca-se aqui que a estratégia proposta encripta sinais complexos em banda base que, quando modulados, dão origem a sinais BPSK, QPSK e 16-QAM. Por simplicidade de notação, adotaremos as nomenclaturas BPSK, QPSK e 16-QAM para os sinais em banda base. No s-AES, são criptografados blocos de 125 símbolos. O software encripta, por meio de DSP, sinais em banda base que podem ser transmitidos por diversos meio de transmissão, desde que seja realizada a modulação em uma portadora adequada.

(3) Na comunicação entre um transmissor e um receptor, o transmissor converte sequências de bits em sinais que são modulados e transmitidos pelos meios de comunicação e o receptor converte os sinais recebidos em sequências de bits. Como visto anteriormente, em criptografia de sinais, as operações são realizadas nos sinais antes de serem modulados e transmitidos pelo meio. Uma vez que esses sinais representam sequências de bits, é possível adotar, em criptografia de sinais, os mesmos requisitos de segurança definidos em criptografia de dados.

(4) Modos de operação são definidos em criptografia de dados para tornar aleatórias as mensagens cifradas e tornar as técnicas de criptografia semanticamente seguras. Um dos modos de operação importantes é o *counter mode* (CTR mode). Um modo de operação análogo a ele, denominado s-CTR (Counter Mode adapted to signals), foi projetado para operar em criptografia de sinais e tornar aleatórios os sinais encriptados.

(5) O processo de reutilização de chaves elimina a necessidade de transmissão de uma nova chave a cada bloco enviado. Em algoritmos clássicos de criptografia, a reutilização da

chave compromete a segurança da técnica pois um invasor pode descobrir informações da chave enviando, por exemplo, a mesma mensagem com apenas um bit diferente. Em criptografia de dados, a reutilização de chaves é possível com a utilização de modos de operações. No melhor de nosso conhecimento, a reutilização de chaves não havia sido implementada em criptografia de sinais até o desenvolvimento desse trabalho. A implementação em software do s-CTR em conjunto ao s-AES aleatoriza os sinais encriptados e dessa maneira, é possível reutilizar as chaves criptográficas com segurança.

1.3 Organização do trabalho

O restante dessa dissertação está organizado da seguinte maneira. O Capítulo 2 aborda os fundamentos da criptografia de dados, a distinção das técnicas de criptografia de dados pela simetria das chaves criptográficas e pelo comprimento das mensagens de entrada, as principais técnicas comerciais utilizadas e os modos de operação utilizados para tornar aleatórias as mensagens cifradas. No Capítulo 3, são abordadas as características e algumas das técnicas de criptografia de sinais estudadas atualmente. A nova técnica proposta, o s-AES, está descrita no Capítulo 4. Os resultados referentes à segurança e à transmissão de sinais encriptados pelo s-AES são discutidos no Capítulo 5. Por fim, as considerações finais desse trabalho são apresentadas no Capítulo 6.

2 Criptografia de dados

Nesse capítulo serão abordados os detalhes operacionais da criptografia de dados, uma estrutura de criptografia utilizada por diversas técnicas comerciais, duas das principais técnicas comerciais e os modos de operação. A Seção 2.1 trata da operação da criptografia de dados e das classificações pela simetria da chave criptográfica e pelo comprimento da chave criptográfica. Na Seção 2.2 são abordadas as Redes de Feistel, que são estruturas de criptografia muito utilizadas por técnicas comerciais, e duas das técnicas mais importantes de criptografia moderna: o DES e o AES. Por fim, na Seção 2.3, são apresentados os modos de operação.

2.1 Operação e classificação da criptografia de dados

Na criptografia de dados conjuntos de bits entre a camada de Enlace (camada 2) e a camada de Aplicação (camada 7) do modelo OSI são processados. Em um processo de encriptação, a mensagem original, m, é encriptada em uma mensagem cifrada, c, em acordo com

$$c = E(m, k_e), \tag{1}$$

em que E é o algoritmo de encriptação e k_e é a chave de encriptação. Um receptor autorizado, em posse da chave de desencriptação, k_d, desencripta a mensagem cifrada, c, na mensagem original, m, por meio de

$$m = D(c, k_d), \tag{2}$$

em que D é o algoritmo de desencriptação e k_d é a chave de desencriptação.

Com relação às chaves, a criptografia de dados pode ser dividida em criptografia simétrica e assimétrica (KATZ; LINDELL, 2014). Em criptografia simétrica, as estações transmissoras e receptoras devem possuir a mesma chave durante a comunicação. A chave utilizada para desencriptar as mensagens é uma função da chave utilizada na encriptação e o receptor calcula a chave a partir da chave do transmissor ou utiliza a chave igual a do transmissor. De fato, usualmente a chave para descriptografar uma mensagem é igual à chave utilizada para criptografar, ou seja, $k_e = k_d$.

Em criptografia assimétrica, também conhecida como criptografia de chave pública, as chaves utilizadas nos processos de encriptação e desencriptação são diferentes. Nesse tipo de criptografia, um par de chaves criptográficas é atribuído a cada estação, uma chave pública e uma chave privada. Para que uma mensagem possa ser encriptada e desencriptada corretamente, é necessário utilizar o par de chaves de determinada estação.

Quando a criptografia assimétrica é utilizada na troca de informações entre duas estações, as mensagens são encriptadas com a chave pública da estação receptora e a estação receptora usa sua chave privada para desencriptar corretamente a mensagem. Essa comunicação é segura pois a informação encriptada com a chave pública de determinada estação só pode ser desencriptada corretamente quando a chave privada dessa mesma estação é utilizada. A criptografia assimétrica também é aplicada para autenticação, em assinaturas digitais por exemplo. Nesse caso, a mensagem é encriptada com a chave privada da estação transmissora e a estação receptora desencripta a mensagem com a chave pública da estação transmissora. Como só é possível desencriptar essa mensagem corretamente com a chave pública da estação que a transmitiu, é possível autenticar que aquela mensagem foi transmitida por determinada estação.

A criptografia assimétrica requer mais processamento computacional que a simétrica e pode ser mais lenta. Atualmente, a criptografia assimétrica é muito utilizada para realizar a troca de chaves em comunicações que utilizam criptografia simétrica. As estratégias de Diffie-Hellman e de River-Shamir-Adleman (RSA) (KATZ; LINDELL, 2014) são duas das mais utilizadas para esse fim.

A criptografia de dados pode ser classificada, além da simetria das chaves, pelo comprimento da mensagem a ser encriptada. As cifras de fluxo encriptam bit por bit de mensagens com comprimento indefinido, enquanto as cifras de bloco dividem a mensagem em blocos de comprimento fixo e encripta cada um deles (MENEZES *et al.*, 1996; PFLEEGER, 2009). Historicamente, cifras de bloco mostram-se mais seguras do que técnicas de cifras de fluxo. Embora ainda existam algumas técnicas comerciais de cifras de fluxo, boa parte das que foram utilizadas tiveram sua segurança quebrada com o tempo (BARKAN; BIHAM; KELLER, 2003; LU; MEIER; VAUDENAY, 2005; WU; PRENEEL, 2006; WU; PRENEEL, 2007).

Uma vez que grande parte dos algoritmos comerciais atuais são de cifra de bloco, voltaremos nossa atenção a estruturas e técnicas de criptografia de dados que sejam baseadas nesse tipo de cifra. Com relação a segurança de cifras de bloco, existem vários

ataques possíveis. Dois dos mais importantes são o ataque de força bruta (*brute-force attack*, BFA) e o ataque de texto escolhido (*chosen plaintext attack*, CPAs).

Em um BFA, o interceptador deve testar todas as possibilidades de texto para garantir que a mensagem seja recuperada corretamente. Como em criptografia de dados a mensagem é composta por bits, o interceptador deve fazer 2 tentativas (0 ou 1) em cada bit do bloco encriptado para recuperar o bloco original sem erros. O número de BFAs, nesse caso, é calculado por

$$N_{ataques} = 2^{n_b}, \tag{3}$$

em que n_b é o número de bits do bloco.

Em um CPA, é realizada uma espécie de jogo entre o interceptador e o algoritmo de encriptação. O interceptador escolhe dois blocos de mensagem, as envia ao algoritmo de encriptação, que encripta as duas mensagens com a mesma chave e envia os dois blocos encriptados ao interceptador. Se o interceptador não consegue distinguir, com probabilidade acima de 50%, qual dos blocos cifrados é resultado da encriptação de determinado bloco original, afirma-se que a técnica tem indistinguibilidade contra CPAs. O conceito de indistinguibilidade foi estabelecido em (GOLDWASSER; MICALI, 1984) e é equivalente a definição de segurança semântica (KATZ; LINDELL, 2014). Ou seja, técnicas que apresentam indistinguibilidade são semanticamente seguras sob CPAs.

Embora existam vários outros ataques possíveis (KATZ; LINDELL, 2014), nesse trabalho nos restringiremos à análise de BFAs e CPAs. A próxima seção abordará uma estrutura de cifras de bloco amplamente utilizada por técnicas de criptografia e dois importantes padrões de criptografia de dados baseados em cifras de bloco.

2.2 Redes de Feistel e técnicas importantes de criptografia

Nesta seção abordaremos as Redes de Feistel, estruturas de criptografia utilizadas por diversas técnicas de criptografia de dados. Também serão abordados o DES e o AES, padrões de criptografia de dados baseados em cifras de bloco amplamente utilizados na criptografia moderna.

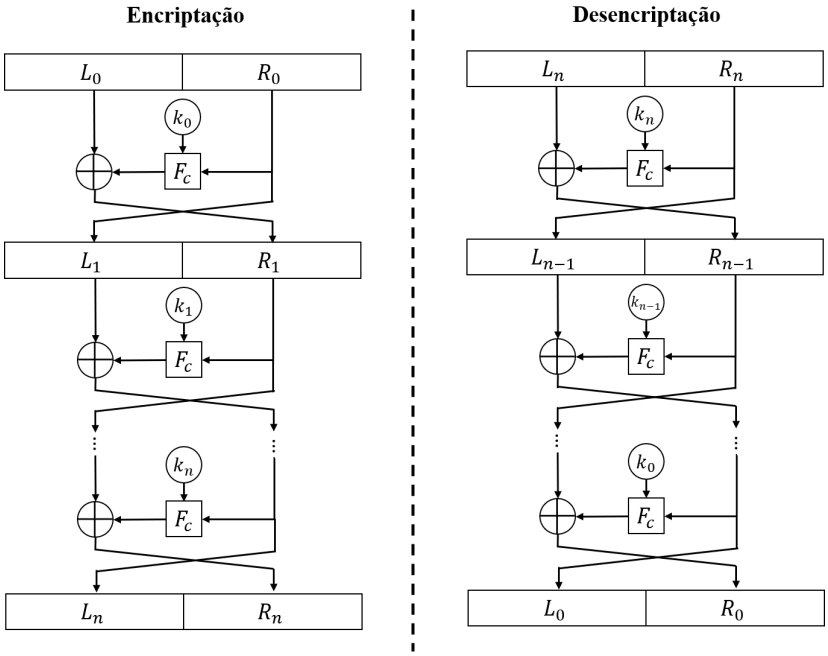


Figura 1 – Esquema das Redes de Feistel.

2.2.1 Redes de Feistel

As Redes de Feistel (MENEZES *et al.*, 1996) são estruturas utilizadas por diversas técnicas comerciais de criptografia de blocos, tais como: DES, TEA (*Tiny Encryption Algorithm*), RC5 (*Rivest Cipher 5*) e outras. Um diagrama de bloco para a operação das Redes de Feistel é apresentado na Fig. 1. O bloco de entrada é dividido em dois conjuntos do bits. Os bits da esquerda, L_0, e os bits da direita, R_0. O conjunto R_0 passa por uma função criptográfica, F_c, com a primeira chave, k_0. Além disso, ele passa a ser o próximo conjunto de bits da esquerda, ou seja, $L_1 = R_0$. O conjunto L_0 passa por uma operação XOR com o produto da função criptográfica entre a primeira chave e o conjunto R_0 e passa a ser o próximo conjunto da direita, R_1. Ou seja, $R_1 = L_0 \oplus F(R_0, k_0)$. As próximas N iterações ocorrem da mesma maneira, em acordo com:

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus F_c(R_i, k_i) \end{aligned} . \tag{4}$$

De maneira geral, as Redes de Feistel realizam um número pré-determinado (definido em acordo com a necessidade do projeto) de iterações em blocos de comprimento fixo. Cada iteração, como mostrado na Fig. 1, conta com uma permutação e uma função criptográfica. Em cada uma das iterações é utilizada uma sub-chave para criptografar os blocos. A

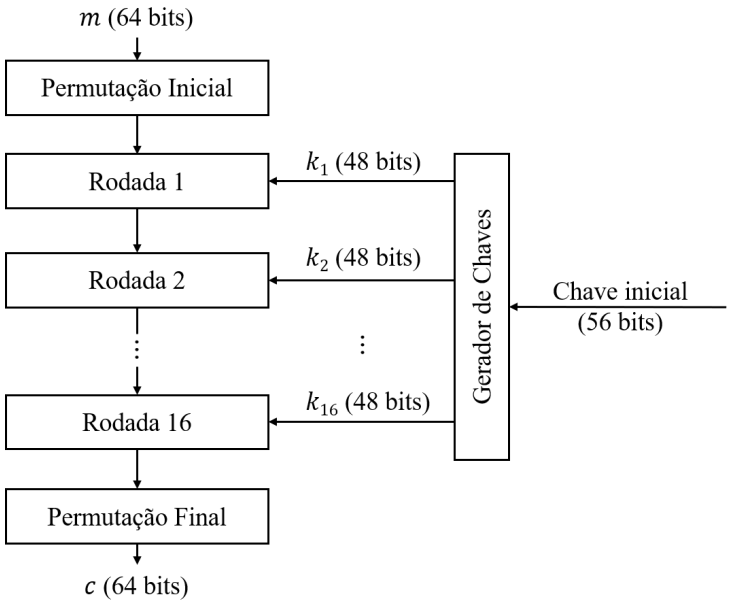


Figura 2 – Diagrama de encriptação do DES.

chave do primeiro bloco pode ser gerada aleatoriamente pelo transmissor e trocada com o receptor. As sub-chaves podem ser geradas utilizando algum algoritmo de expansão de chaves no transmissor e no receptor a partir da primeira.

Uma das vantagens de utilizar as Redes de Feistel é a inversibilidade da estrutura (SCHNEIER, 1996; STINSON; PATERSON, 2018). O algoritmo de desencriptação funciona do mesmo modo que o de encriptação, apenas invertendo a ordem das chaves criptográficas, ou seja: $k_n, k_{n-1}, ..., k_0$. A inversibilidade da estrutura das redes de Feistel não depende da função criptográfica, ou seja, mesmo que a função criptográfica aplicada não seja inversível, as Redes de Feistel continuam sendo inversíveis. Como mencionado anteriormente, vários padrões comerciais de criptografia são baseados em Redes de Feistel. Um exemplo desses padrões, o DES, será abordado na próxima seção.

2.2.2 DES

O DES é um padrão de criptografia simétrica de dados publicado pelo *National Institute of Standards and Technology* (NIST) em 1973 (PUB, 1977). A Fig. 2 mostra o diagrama de encriptação adotado pelo DES. O DES encripta blocos de 64 bits utilizando chaves criptográficas com comprimento de 56 bits. A estrutura desse padrão foi desenvolvida para conferir as propriedades de difusão e confusão às mensagens cifradas (FOROUZAN, 2007). O algoritmo de encriptação consiste em uma permutação inicial, dezesseis rodadas

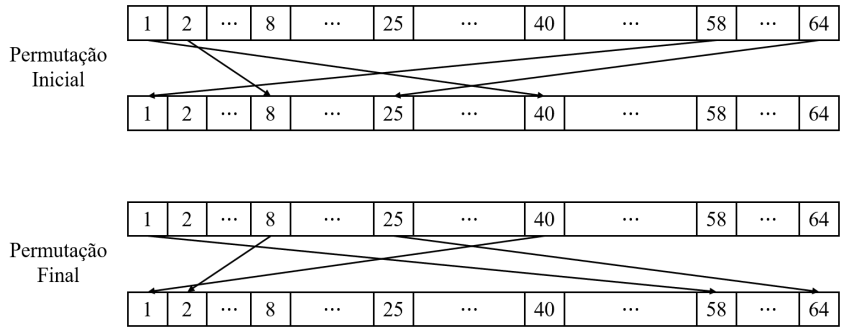


Figura 3 – Operações de permutação do DES.

de uma Rede de Feistel e uma permutação final. As chaves utilizadas em cada rodada da Rede de Feistel têm 48 bits e são geradas por meio da chave inicial de 56 bits por um gerador de chaves.

O bloco da mensagem de entrada passa por uma permutação inicial. Em seguida o bloco é dividido em duas partes de 32 bits e passa por 16 rodadas, chamadas de rodadas de Feistel. Em cada rodada de Feistel, uma função criptográfica é aplicada à parte direita do bloco (veja 2.2.1). No DES, a função utilizada na Rede de Feistel é denominada função DES. Uma chave, k_i, de 48 bits é aplicada a R_i, de 32 bits, em que i corresponde à i-ésima rodada de Feistel. A saída gerada pela função DES tem comprimento de 32 bits. Após as dezesseis rodadas de Feistel, é realizada uma Permutação Final e então, o bloco está criptografado.

As operações de permutação inicial e final trocam a ordem dos bits de maneira pré-definida e sem utilizar chaves. Os bits de entrada da permutação inicial são permutados de acordo com uma regra pré-estabelecida. A permutação final é a operação inversa da permutação inicial. A Fig. 3 ilustra algumas das permutações realizadas.

O diagrama da função DES é apresentado na Fig. 4. Como a parte direita do bloco, R_i, têm 32 bits e a chave criptográfica têm 48 bits, a primeira etapa da função DES é realizar uma expansão do bloco R_i para que esse tenha o mesmo tamanho da chave. A operação detalhada da função de expansão não faz parte do escopo dessa dissertação, mas pode ser encontrada em (FOROUZAN, 2007). Após esse processo, é realizada uma XOR entre o R_i expandido e a chave. O próximo passo da função DES é realizar uma operação de substituição nos bits. Essa operação utiliza tabelas de substituição (*Substitution boxes*, S-boxes) calculadas previamente para substituir os bits. São utilizadas 8 S-boxes para conferir a propriedade de confusão às mensagens cifradas. Cada S-box tem 6 bits de entrada

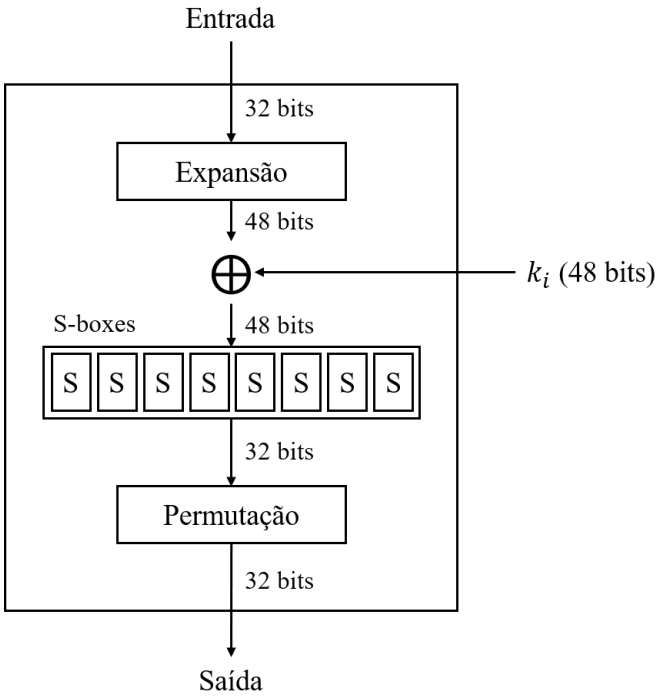


Figura 4 – Função DES.

e 4 de saída, ou seja, após essa etapa, o comprimento do sub-bloco volta a ser 32 bits. Por fim, uma última permutação pré-definida é realizada.

Alguns pontos negativos do DES foram encontrados com o passar dos anos. O principal deles é o tamanho da chave. Com apenas 56 bits de comprimento de chave, o número de BFAs é igual a $2^{56} \approx 10^{16}$. Com o poder computacional disponível em 1988, foi possivel quebrar a segurança do DES em 56 horas (GILMORE, 1998). Assim, a partir do final da década de 90 até o início da década de 2000 foi realizada uma chamada pública para o recebimento de propostas de um novo padrão de criptografia que fosse seguro. Em decorrência dessa chamada pública, em 2001 foi publicado o padrão AES, que será discutido na próxima seção.

2.2.3 AES

O *Advanced Encryption Standard* (AES) é um padrão de cifra de bloco simétrica desenvolvido por Vincent Rijmen e Joan Daemen em 2001 (RIJMEN; DAEMEN, 2001; FIPS, 2001). É um padrão de cifra de blocos seguro e muito utilizado atualmente. O algoritmo do AES conta com múltiplas rodadas para encriptar blocos com comprimento de 128 bits. O número de rodadas necessárias para prover as propriedades de difusão

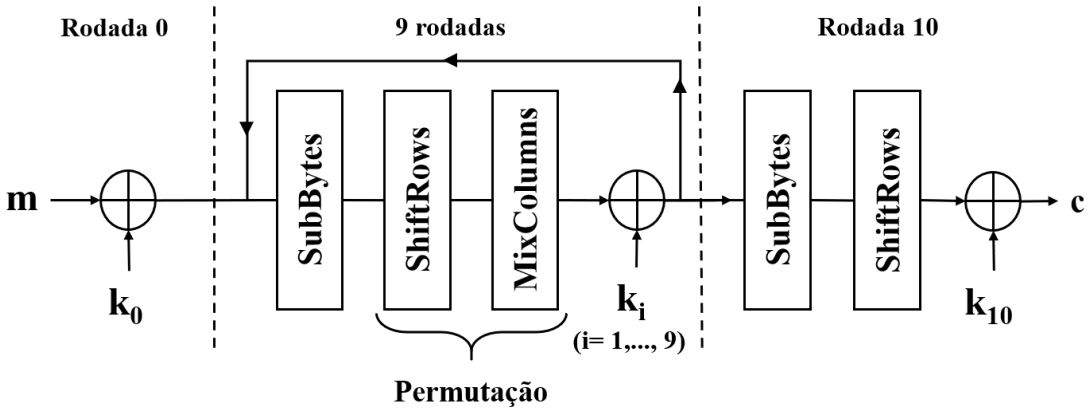


Figura 5 – Esquema do AES para blocos de 128 bits.

e confusão aos blocos cifrados varia com o tamanho da chave criptográfica. Os padrões estabelecidos para o AES utilizam chaves com comprimento igual a 128 (AES-128), 192 (AES-192) e 256 (AES-256). O número de rodadas utilizadas para cada um desses padrões são 10, 12 e 14, respectivamente. A maioria das aplicações comerciais utilizam o AES-128 e o governo dos Estados Unidos utiliza o AES-256 para aplicações ultrassecretas.

O padrão AES-128 é o mais utilizado atualmente, logo, nosso interesse recai sobre ele. Como dito anteriormente, são encriptados blocos com 128 bits e 10 rodadas são utilizadas para conferir difusão e confusão aos blocos encriptados. O diagrama da Fig. 5 ilustra o funcionamento do AES-128. Cada bloco de entrada, m, é interpretado como uma matriz quadrada de 16 bytes (4 bytes x 4 bytes). Essa interpretação é necessária para realizar as operações de permutação utilizadas (deslocamento de linhas e mistura de colunas).

Inicialmente, o bloco de entrada passa por uma XOR com a primeira chave criptográfica, k_0. Em seguida, o bloco passa por 9 rodadas em que são realizadas uma substituição de bytes (SubBytes), um deslocamento das linhas (ShiftRows) da matriz, uma mistura de colunas (MixColumns) e uma XOR com a chave da rodada, k_i. Após as 9 rodadas, a última rodada conta com uma substituição de bytes, um deslocamento de linhas e uma XOR com a última chave criptográfica, k_{10}. As 10 chaves criptográficas utilizadas nas 10 rodadas do AES-128 são expandidas a partir da primeira chave, k_0, por meio de um algoritmo de expansão de chaves encontrado em (FIPS, 2001).

Para o entendimento das operações SubBytes, ShiftRows e MixColumns, faz-se necessária uma breve explicação acerca de Corpos de Galois (*Galois Field*) (LIDL; NIEDERREITER, 1994). O Corpo de Galois é um conjunto finito de p^n elementos, em que

p é um número primo e n é um número inteiro positivo. O corpo finito $\{0, 1, 2, \ldots, p^n - 1\}$, por exemplo, é um Corpo de Galois. A notação utilizada para representar um Corpo de Galois é GF(p^n), em que o número p^n é a ordem do corpo. Como as operações utilizadas no AES são baseadas no corpo de Galois, podemos interpretar cada byte do AES como um elemento de um corpo com ordem 2^8, ou seja, um corpo GF(2^8).

As operações entre os elementos de um Corpo de Galois devem resultar em um elemento que esteja dentro do próprio corpo. Logo, as operações que são realizadas entre números reais devem ser redefinidas de maneira conveniente. Limitaremo-nos à definição das operações de adição e multiplicação no corpo GF(2^8) (WAGNER, 2003), corpo em que se baseiam as operações do AES. Porém, essas operações podem ser redefinidas para um corpo de ordem p^n.

- **Adição:**

  A adição de dois elementos no corpo GF(2^8) é definida pela soma em módulo 2 (0+0 = 0; 0+1=1; 1+0=1; 1+1 = 0) e equivale a uma operação XOR. Os dígitos de um byte podem ser expressos como coeficientes de um polinômio. Por exemplo, o byte 10110011 pode ser representado como $1 \cdot x^7 + 0 \cdot x^6 + 1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0$. Assim, para realizar a soma de dois bytes no GF(2^8), deve-se fazer a soma módulo 2 dos coeficientes dos polinômios que representam esses bytes.

- **Multiplicação:**

  É realizada a multiplicação dos polinômios que representam os elementos em módulo g, em que g é um polinômio binário irredutível de grau 8. Um polinômio é dito irredutível se os únicos divisores dele são 1 e ele mesmo. Supondo a multiplicação entre dois elementos, e_1 e e_2, temos

$$y(x) = e_1(x) \cdot e_2(x) \mod g(x), \tag{5}$$

  em que $a \mod b$ representa o resto da divisão entre a e b. No padrão AES, o polinômio irredutível utilizado é $g(x) = x^8 + x^4 + x^3 + x + 1$.

  Por exemplo, realizaremos a multiplicação entre o byte 10110110 e o byte 01010011 (WAGNER, 2003). Devemos, primeiro, realizar a multiplicação entre os dois bytes e depois dividir pelo polinômio irredutível g. É possível realizar todos os cálculos baseando-se nos polinômios que representam os bytes. A multiplicação desses dois

bytes em um corpo de Galois com polinômio irredutível $g(x) = x^8 + x^4 + x^3 + x + 1$ é 00011011.

A partir desse conhecimento introdutório sobre Corpos de Galois, é possível especificar as operações SubBytes, ShiftRows e MixColumns.

2.2.3.1 SubBytes

A substituição de bytes (SubBytes) é uma operação não linear realizada por meio de uma transformação afim sobre o corpo GF(2^8) (SINGH; AGARWAL; CHAND, 2017). Cada byte do bloco de entrada da operação é substituído por outro, b', em acordo com

$$b' = Ab \oplus c_a \mod g(x), \tag{6}$$

em que A representa a matriz afim utilizada pela operação, b é o inverso multiplicativo do byte que se deseja substituir, c_a é a constante afim 0x63 (01100011) e $g(x)$ é o polinômio irredutível $x^8 + x^4 + x^3 + x + 1$. A substituição dos bytes (SINGH; AGARWAL; CHAND, 2017) pode ser descrita, após o desenvolvimento de (6), por

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \tag{7}$$

Para otimizar a substituição e não ser necessário calcular a transformação descrita em (6) sempre que um byte for passar pela operação, a tabela de substituição (S-box) é utilizada. Essa tabela é construída com todos os valores de transformações possíveis. A S-box utilizada no AES é ilustrada na Tabela 1 (SINGH; AGARWAL; CHAND, 2017). Um byte pode ser representado, em notação hexadecimal, por XY. Dessa maneira, X é o caractere que representa os 4 primeiros bits e Y os 4 últimos bits. Cada byte XY será substituído pelo byte que for a intersecção do *nibble* (conjunto de 4 bits) da linha X com o

Tabela 1 – S-Box para o padrão AES-128.

		X														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Y	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

nibble da coluna Y nessa tabela. Essa operação não linear de substituição é a responsável por conferir a propriedade de confusão aos blocos encriptados.

2.2.3.2 ShiftRows

O deslocamento de linhas (ShiftRows) (DAEMEN; RIJMEN, 2013) é uma das operações de permutação realizadas no AES. As linhas da matriz (4 bytes x 4 bytes) do bloco são deslocadas ciclicamente em bytes. A Fig. 6 ilustra o funcionamento da operação. A matriz de entrada pode ser denominada como matriz s e, após a operação, pode ser denominada matriz s'. Cada byte da matriz s pode ser denominado como $s_{r,c}$ em que o subscrito r diz respeito ao número da linha da matriz em que o byte se encontra e c diz respeito ao número da coluna.

Os bytes da primeira linha da matriz s não passam por nenhum deslocamento. Logo, a primeira linha da matriz s' é igual à primeira linha da matriz s. Na segunda linha, é realizado o deslocamento de um byte. O primeiro byte da segunda linha da matriz s passa a ser o último byte da segunda linha da matriz s' e todos os outros dessa linha são deslocados em um byte à esquerda. Na terceira linha ocorre o deslocamento de dois bytes à esquerda e na quarta linha, três bytes são deslocados à esquerda.

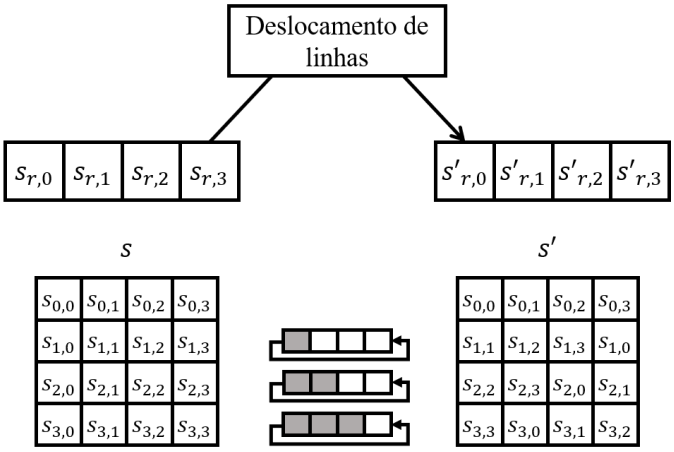


Figura 6 – Deslocamento de linhas (ShiftRows).

2.2.3.3 MixColumns

A mistura de colunas (MixColumns) (DAEMEN; RIJMEN, 2013) é a segunda operação de permutação realizada pelo AES. Cada uma das colunas da matriz do bloco passa pelo processo de mistura da colunas. A coluna de entrada da operação pode ser denominada como w e a coluna de saída como w'. Os bytes da coluna de entrada serão denominados como w_i, em que o subscrito i indica a linha do byte. Já os bytes da coluna de saída são denominados como w'_i.

Os bytes w'_i são calculados a partir da multiplicação entre uma matriz conhecida e os bytes w_i. Essa operação é dada por

$$\begin{bmatrix} w'_0 \\ w'_1 \\ w'_2 \\ w'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{bmatrix}. \tag{8}$$

As operações ShiftRows e MixColumns são, juntas, responsáveis por prover difusão aos blocos encriptados. Além disso, junto com a operação de substituição, essas operações formam a rede de substituição e permutação (*substitution-permutation network*, SPN).

Para quebrar o AES-128 por BFA são necessárias $2^{128} \approx 10^{38}$ tentativas. O ataque mais eficiente a esse tipo de encriptação reduz o número de tentativas a $2^{126} \approx 10^{37}$, ou seja, apenas 2 dos 128 bits do bloco não devem ser testados, o que evidencia a segurança do AES (BOGDANOV; KHOVRATOVICH; RECHBERGER, 2011). Já no AES-256, o número de BFAs é igual à $2^{256} \approx 10^{77}$.

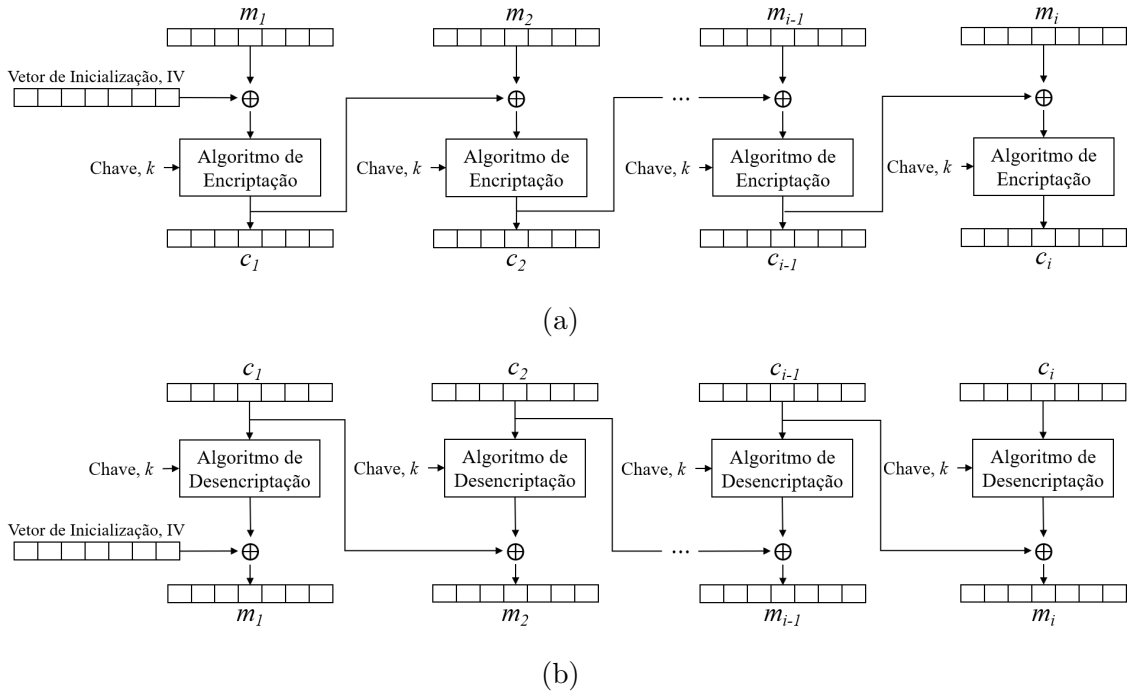


Figura 7 – Diagrama de (a) encriptação e (b) desencriptação do modo de operação CBC.

2.3 Modos de Operação

Os algoritmos de encriptação de dados discutidos na Seção 2.2 não são robustos contra CPAs. É necessária, então, a utilização de algoritmos que tornam aleatórias as mensagens cifradas. Os modos de operação foram criados para que as técnicas de criptografia existentes sejam utilizadas de maneira que blocos cifrados por blocos de entrada idênticos sejam diferentes (KATZ; LINDELL, 2014). Além disso, eles possibilitam a reutilização das chaves criptográficas de maneira segura. Alguns dos principais modos de operação são abordados a seguir.

2.3.1 *Cipher Block Chaining Mode* (CBC Mode)

A cifra de blocos encadeados (*Cipher Block Chaining*, CBC) é um modo de operação em que os blocos são encriptados de maneira sequencial de forma que a encriptação de cada bloco depende do bloco cifrado anterior (KATZ; LINDELL, 2014). A Fig. 7 (a) mostra o diagrama de encriptação do modo CBC. É realizada uma XOR entre o primeiro bloco de entrada, m_1 e um vetor de inicialização (*Initialization Vector*, IV), que pode ser divulgado publicamente ou enviado pelo transmissor ao receptor no início da comunicação.

Na sequência, o resultado dessa operação é encriptado por alguma técnica de criptografia de dados. Temos então, o primeiro bloco cifrado, c_1. O bloco c_1 é utilizado no processo de criptografia do bloco subsequente, m_2. No processo de criptografia do bloco m_2, uma XOR é realizada entre m_2 e o bloco $c1$ e o produto dessa operação é encriptado. Esse processo acontece sequencialmente de forma que o bloco m_i sempre passa por uma XOR com o bloco c_{i-1} e o resultado dessa operação é encriptado para dar origem ao bloco c_i.

O diagrama de desencriptação do CBC é apresentado na Fig. 7 (b). Os blocos cifrados passam primeiro pelo algoritmo de encriptação e depois por uma XOR com o bloco cifrado anterior. No primeiro bloco, a XOR é realizada com o mesmo vetor de inicialização utilizado no processo de encriptação.

No caso em que dois blocos iguais são encriptados com a mesma chave, os blocos cifrados são diferentes pois cada um dos blocos passará por uma XOR com uma informação diferente. O modo CBC utiliza processamento em série, o que significa que cada bloco só pode ser processado depois que o bloco anterior a ele já tiver sido processado. Essa característica faz com que esse modo de operação seja mais lento que outros modos de operação disponíveis.

Com relação à integridade dos dados, se existir algum bit errado em um bloco de entrada, o erro desse bit vai ser propagado para todos os blocos cifrados subsequentes. Enquanto isso, se na transmissão dos dados um bit do bloco cifrado for perdido, o erro desse bit vai influenciar apenas dois blocos.

2.3.2 *Output Feedback Mode* (OFB Mode)

O modo de feedback de saída (*Output Feedback Mode*, OFB mode) também é um modo de operação serial, em que a encriptação de um bloco depende diretamente do bloco anterior (KATZ; LINDELL, 2014). A Fig. 8(a) mostra o diagrama de encriptação do modo OFB. Um vetor de inicialização é encriptado por alguma técnica de criptografia. O resultado dessa operação passa por uma XOR com o bloco de entrada, m_1, para gerar o bloco cifrado c_1. Além disso, o resultado da XOR também será a entrada da técnica de criptografia no processo de encriptação do bloco subsequente.

A Fig. 8(b) mostra o diagrama de desencriptação do modo OFB. É importante destacar que o algoritmo de encriptação da técnica que for utilizada no modo OFB será

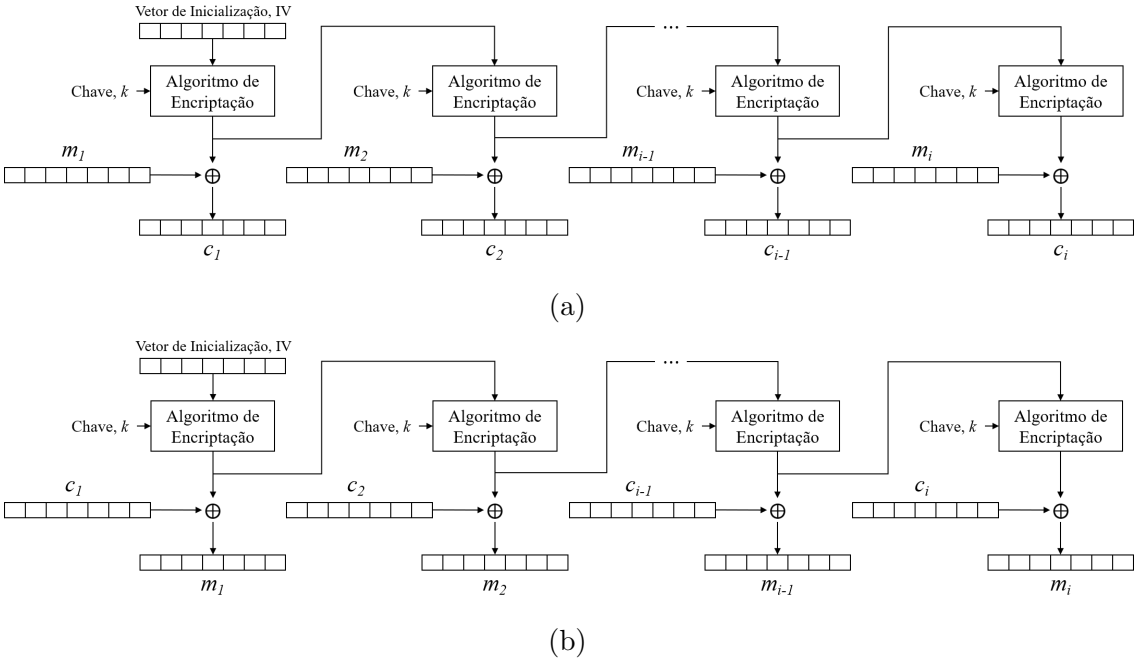


Figura 8 – Diagrama de (a) encriptação e (b) desencriptação do modo de operação OFB.

utilizado tanto na encriptação quanto na desencriptação dos blocos. Isso ocorre pois a técnica não é utilizada para encriptar os blocos de dados.

Observa-se que o resultado da encriptação de dois blocos de entrada iguais será dois blocos cifrados diferentes. Com relação à integridade, o erro de um bit no bloco de entrada não é propagado para nenhum bloco. A ocorrência de erros nos bits dos blocos cifrados também não é propagada na desencriptação dos blocos. Uma das desvantagens do modo OFB é que, assim como o CBC, ele tem processamento serial e não é possível utilizar vários processadores para encriptar paralelamente diversos blocos.

2.3.3 *Counter Mode* (CTR Mode)

O *Counter Mode* (CTR Mode) é um modo de operação em que a encriptação de cada bloco não depende do bloco anterior (KATZ; LINDELL, 2014). A Fig. 9(a) mostra o diagrama de encriptação do modo CTR. O bloco de entrada, β_i, é composto por duas partes. A primeira parte é o *nonce*, um bloco binário aleatório e a segunda é o *counter*, um contador que é incrementado a cada bloco encriptado. Na encriptação do primeiro bloco, m_1, o bloco de entrada β_1 é encriptado por alguma técnica de encriptação. O produto dessa operação passa por uma XOR com o bloco m_1, gerando o primeiro bloco cifrado, c_1. Genericamente, o bloco cifrado é dado por $c_i = m_i \oplus E(\beta_i, k)$.

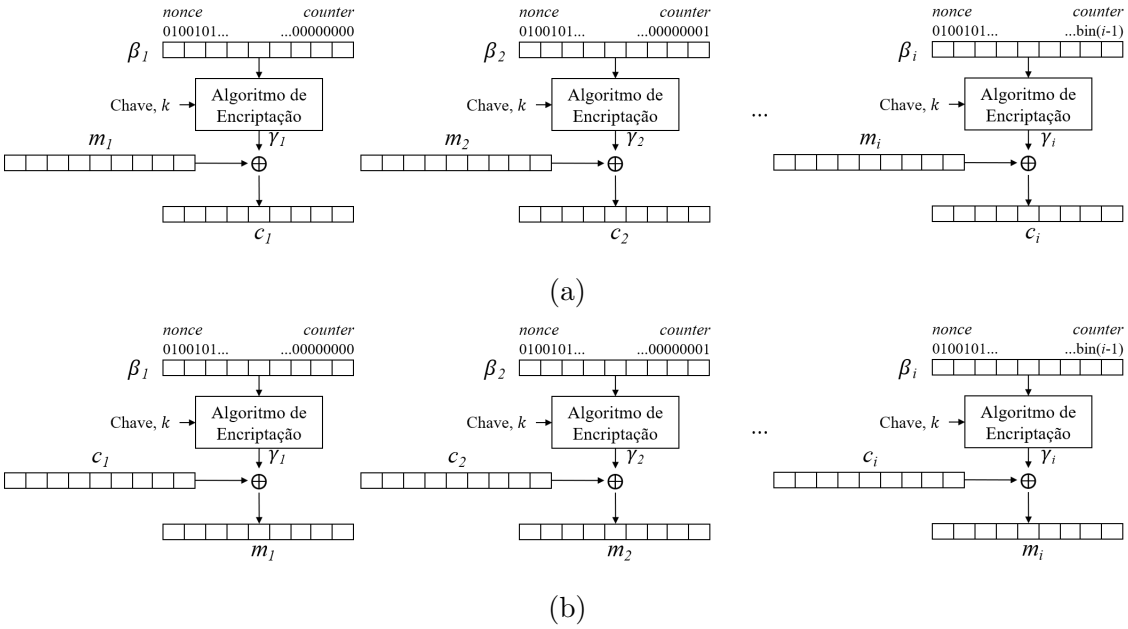


Figura 9 – Diagrama de (a) encriptação e (b) desencriptação do modo de operação CTR.

A Fig. 9(b) mostra o algoritmo de desencriptação do modo CTR. A desencriptação é muito similiar à encriptação. A diferença é que nessa, a XOR é realizada entre o bloco cifrado e o bloco γ_i. Assim como no modo OFB, os blocos de mensagem não passam pela técnica de encriptação. O objetivo de aplicar a técnica ao bloco β_i é criar uma sequência de bits aleatória que, quando aplicada à XOR com o bloco m_i, confira difusão e confusão. De fato, se o algoritmo de encriptação utilizado for projetado de maneira satisfatória, a mudança de um bit no bloco β_i ou na chave k vai ocasionar a mudança de aproximadamente 50% dos bits do bloco γ_i.

Qualquer possível erro de bit nos blocos de entrada ou cifrados não é propagados para nenhum outro bloco. Além disso, o CTR tem operação paralela, o que permite que vários processadores encriptem ou desencriptem simultaneamente inúmeros blocos.

Concluindo o Capítulo 2, observa-se que uma das preocupações na evolução da criptografia de dados foi conseguir desenvolver técnicas seguras que utilizassem chaves curtas, pois é inviável trocar a chave entre o transmissor e o receptor quando a chave tem o mesmo tamanho da mensagem a ser transmitida. As cifras de blocos possibilitaram utilizar chaves menores que o tamanho da mensagem e os modos de operação viabilizaram que a mesma chave fosse utilizada por diversos blocos. É importante observar que um padrão de criptografia não garante segurança para sempre, o avanço computacional possibilita que a segurança de padrões de criptografia sejam quebrados e por consequência, novos padrões

devem ser criados para manter as comunicações seguras. Embora a segurança das redes de Feistel e do padrão DES tenham sido quebradas, o AES é um padrão que ainda é seguro nos dias atuais.

3 Criptografia de sinais

A criptografia de sinais, também conhecida como criptografia na camada física (*physical layer encryption*, PLE), pode ser complementar e até mais segura que a criptografia de dados. Técnicas de PLE atuam nos sinais convertidos pela camada física (camada 1) do modelo OSI. Se a criptografia de sinais for bem sucedida, interceptadores não devem conseguir identificar corretamente os sinais que estão sendo transmitidos pelo meio de transmissão. Para isso, os sinais encriptados devem ser similares a ruído e possuir taxa de erro de bit (*bit error rate*, BER), idealmente, igual a 0,5. Receptores autorizados, em posse da chave criptográfica, devem recuperar o sinal original com a menor BER possível. Nas próximas seções discutiremos as características principais de algumas das técnicas utilizadas para prover confidencialidade na camada física.

3.1 Esteganografia

Uma das técnicas para prover confidencialidade é a esteganografia óptica (WANG; PRUCNAL, 2010; WU *et al.*, 2013). Embora não seja considerada uma técnica de criptografia porque o sinal não é submetido à operações de criptografia, a esteganografia é uma técnica interessante de transmitir sinais com confidencialidade. Nessa técnica, os sinais são transmitidos com níveis de potências inferiores aos do ruído do canal. Dessa maneira, um interceptador não é capaz de notar a presença de transmissão em determinado canal. O receptor autorizado deve recuperar os níveis de potência originais do sinal e compensar as distorções provenientes do canal de transmissão.

Embora seja uma ideia interessante transmitir sinais por um meio sem que interceptadores percebam, sinais com níveis muito baixos de potência ficam mais suscetíveis a efeitos degradantes do canal. Todo sinal transmitido por um canal de comunicação está suscetível à efeitos degradantes. Em particular, sinais esteganografados propagados por meios ópticos guiados com outros sinais convencionais estão suscetíveis a efeitos degradantes não lineares, como a mistura de quatro ondas e a modulação de fase cruzada, e a efeitos lineares, como o acúmulo de ruído de emissão espontânea amplificada (*amplified spontaneous emission, ASE*). Porém, os baixos níveis de potência de sinais esteganografados torna muito difícil a compensação desses efeitos pelo receptor.

3.2 Criptografia Quântica

A criptografia quântica é uma das estratégias mais seguras de criptografia pois permite que os envolvidos na comunicação monitorem as características do sinal de maneira que é possível notar a presença de interceptadores (EKERT, 1991; BENNETT; BRASSARD, 1984; BENNETT; BRASSARD; EKERT, 1992; BENNETT *et al.*, 1992). Um canal de comunicação quântica é baseado na transmissão e recepção de partículas quânticas individuais. As partículas quânticas podem ser, por exemplo, elétrons e fótons. Técnicas de criptografia quântica tem como partícula quântica o fóton, logo, nosso interesse recai sobre ele. O fóton é uma partícula fundamental associada à quantização do campo eletromagnético e a direção da oscilação dessa partícula é conhecida como polarização do fóton. Para que um fóton seja medido, ele é absorvido pelo dispositivo de medida. Dessa maneira, um invasor que meça os fótons transmitidos, precisará transmitir outros fótons no canal para que a comunicação não seja interrompida. Pelo teorema da não clonagem (*non-cloning theorem*) (WOOTTERS; ZUREK, 1982) um estado quântico não pode ser clonado, portanto, o invasor não conseguiria inserir no canal fótons iguais aos que ele mediu. O transmissor e o receptor conseguem, então, notar a presença de um invasor no canal.

Um dos protocolos de comunicação quântica mais utilizados é o BB84 (BENNETT; BRASSARD, 1984), proposto por Bennet e Brassard em 1984, utiliza um canal quântico e um canal público clássico para realizar a comunicação entre o transmissor e receptor, denominados Alice e Bob, respectivamente. O canal público é utilizado para Alice e Bob discutirem e compararem os sinais enviados pelo canal quântico. No primeiro passo, Alice envia uma sequência de fótons com polarizações aleatórias (0°, 45°, 90° ou 135°). Bob recebe os fótons e escolhe, aleatoriamente, entre medir cada um deles de acordo com uma de duas bases de medidas de polarização. Uma das bases é denominada retilínea (0°ou 90°, que podem ser interpretados como bit 0 e bit 1, respectivamente) e a outra é denominada diagonal (45°ou 135°, que podem ser interpretados como bit 0 e bit 1, respectivamente). Após a medida, Bob divulga publicamente o a base de medida utilizada, mas não divulga o resultado da medida (0°, 45°, 90° ou 135°). Alice diz a Bob, por meio do canal público, quais fótons ele acertou a medida. Alice e Bob desconsideram a informação de todos os fótons em que uma medida errada foi realizada. Um último teste para verificar a presença

de um interceptador é, então, realizado: Alice e Bob comparam publicamente uma parte dos fótons polarizados que foram medidos corretamente por Bob. Os fótons utilizados para comparação são desconsiderados. Se houver algum erro nesse teste, é muito possível que um interceptador tenha medido determinados fótons e transmitidos outros, então todos os fótons são desconsiderados e o processo é iniciado novamente. Caso contrário, os fótons remanescentes são interpretados como bits. Fotóns com polarização de 0° ou 45° podem ser interpretados como 0's e fótons com polarização de 90° ou 135° interpretados como 1's.

Existe uma diferença importante entre a comunicação óptica clássica e a comunicação óptica quântica. Na comunicação óptica clássica são transmitidos diversos fótons simultaneamente para representar uma unidade de informação. Mesmo que as propriedades degradativas da fibra absorvam alguns dos fótons, a informação ainda chega no receptor de maneira satisfatória. Por outro lado, na comunicação óptica quântica, apenas um fóton é utilizado para representar uma unidade de informação. Se esse fóton for absorvido pelas propriedades físicas da fibra, a informação é perdida. Essa característica faz com que, em criptografia quântica, seja necessário transmitir vários fótons em sequência para garantir que pelo menos um chegue ao receptor de maneira satisfatória. Esse processo faz com que a comunicação óptica quântica opere taxas de transmissão muito inferiores que as taxas de transmissão da comunicação óptica clássica.

Embora a comunicação quântica seja bastante segura, as baixas taxas de transmissão inviabilizam a utilização dessa técnica em sistemas de comunicações atuais. De fato, as taxas alcançadas em criptografia com comunicação quântica são da ordem de 1.3 Mbps (ZHANG *et al.*, 2009; LUCAMARINI *et al.*, 2018) enquanto as redes de comunicação atuais operam, tipicamente, com taxas da ordem de 50 Gbps em cada uma das duas polarizações, totalizando 100 Gbps.

Embora a criptografia quântica não opere em taxas altas de transmissão, as taxas providas são suficientes para transmitir chaves criptográficas. A troca de chaves entre o transmissor e o receptor é de extrema importância e deve ser realizada de maneira tão segura quanto possível. Portanto, a criptografia quântica pode ser aplicada para esse fim. O protocolo BB84, assim como a maioria dos protocolos de comunicação quântica, é utilizado para realizar a troca de chaves criptográficas entre o transmissor e o receptor.

A distribuição quântica de chaves (*quantum key distribution*, QKD) conta atualmente com diversas estratégias. Além do BB84, outro protocolo bastante utilizado é o

E91, proposto por Artur Ekert em 1991 (EKERT, 1991). Esse protocolo baseia-se no emaranhamento quântico (*Quantum Entanglement*).

Existem também algumas técnicas propostas recententemente visando que a QKD seja compatível com os sistemas atuais de comunicação. Em (YIN *et al.*, 2016), é proposto um equipamento para medida dos fótons que possibilita a troca de chaves em um enlace de 404 km. Porém, nesse caso, o receptor precisa estar resfriado a -271 °C. Em (MAO *et al.*, 2018), é proposta a integração entre a estratégia QKD com uma taxa de chave de 4,5 kbps e uma rede comercial com taxa de transmissão de 3,6 Tbps. Já em (LIAO *et al.*, 2017), é proposta uma rede quântica global por meio de satélites. Em uma demonstração com um único satélite foram alcançadas taxas de chave na ordem de kilobits por segundo em distâncias de 1200 km. A empresa suíca ID Quantique tem em seu portfólio alguns dispositivos comerciais para realizar a QKD. O Clavis^3 QKD for R&D e o Cerberis^3 QKD System são dispositivos que operam com uma taxa de chave igual a 1,4 kb/s com uma distância máxima de 75 km, enquanto o Clavis^{300} Quantum Cryptography Plataform opera com uma taxa de chave igual a 6 kb/s com uma distância de até 70 km.

3.3 Criptografia Caótica

A criptografia caótica é uma abordagem que utiliza sistemas caóticos para realizar a encriptação de sinais. Em algumas técnicas, denominadas técnicas de criptografia caótica, sinais modulados são gerados a partir de sistemas caóticos (KE *et al.*, 2016; HOU *et al.*, 2016; YI *et al.*, 2018). Por outro lado, em criptografia digital caótica, sistemas caóticos são utilizados para realizar operações de criptografia em sinais em banda base por meio de DSP (ODEN *et al.*, 2017; GENG *et al.*, 2018; HU *et al.*, 2015; YANG *et al.*, 2016; SULTAN *et al.*, 2018). Nessa dissertação, o interesse recai sobre a criptografia de sinais em banda base, portanto, discutiremos as técnicas de criptografia digital caótica.

Em criptografia caótica digital, são utilizados sistemas caóticos multidimensionais para encriptar os sinais. Um sistema caótico multidimensional é descrito por algumas equações diferenciais e por condições iniciais. Uma chave criptográfica trocada entre o transmissor e o receptor corresponde às condições iniciais do sistema caótico digital. As sequências resultantes da resolução das equações diferenciais dos sistemas caóticos são utilizadas para realizar as operações de encriptação no sinal de entrada. Como exemplos de

técnicas de criptografia caótica digital, discutiremos as técnicas apresentadas em (YANG *et al.*, 2016) e (SULTAN *et al.*, 2018), ambas realizadas em sinais com multiplexação por divisão em frequências ortogonais (*orthogonal frequency domain multiplexing*, OFDM).

A técnica proposta em (YANG *et al.*, 2016) utiliza um sistema hiper-caótico de 4 dimensões para realizar operações de sincronização dos símbolos, permutação em frequência, permutação em tempo e rotação de fase em sinais 16-QAM OFDM com taxa de 8,9 Gbps. Os sinais encriptados são transmitidos por fibras ópticas de 20 km. O sistema de equações utilizado é dado por

$$\begin{cases} \dot{x} = t_1(-x + y) + yzu \\ \dot{y} = t_2(x + y) - xzu \\ \dot{z} = t_3 y - u + t_4 xyu \\ \dot{u} = -t_5 u + xyz \end{cases}, \tag{9}$$

em que t_1, t_2, t_3, t_4 e t_5 são constantes. Pode-se mostrar que a escolha de $t_1 = 35$, $t_2 = 10$, $t_3 = 80$, $t_4 = 0,85$ e $t_5 = 10$ implica em um expoente máximo de Lyapunov positivo, indicando que o sistema apresentará características caóticas. As sequências x, y, z e u são obtidas por meio da resolução do sistema (9) e são utilizadas para encriptar os sinais.

A Fig. 10 mostra o diagrama de blocos do processo de encriptação. Os dados de entrada passam por um conversor série paralelo e, em seguida são mapeados em um sinal 16-QAM. A chave criptográfica é composta pelas condições iniciais utilizadas no sistema de caótico, que gera as sequências x, y, z e u. Na primeira etapa de encriptação, a sequência x é utilizada como uma sequência de treinamento dos símbolos OFDM. A seguir, é realizada uma permutação em frequência dos símbolos OFDM utilizando a sequência y. O sinal OFDM passa por uma transformada rápida inversa de Fourier (*inverse fast Fourier transform*, iFFT) e uma permutação em tempo dos símbolos OFDM é realizada utilizando a sequência z. A última fase de encriptação consiste em utilizar a sequência caótica z para realizar uma rotação em fase dos símbolos. Por fim, o sinal é serializado e o prefixo cíclico é adicionado.

Com relação à segurança da técnica, o sistema de equações caóticas tem sensibilidade às condições iniciais da ordem de $\approx 10^{-15}$. Logo, um erro dessa ordem na chave criptográfica impede que o sinal seja recuperado corretamente. Considerando que o número de subportadoras OFDM seja N_{sub} e o de símbolos seja N_{simb}, a permutação de símbolos

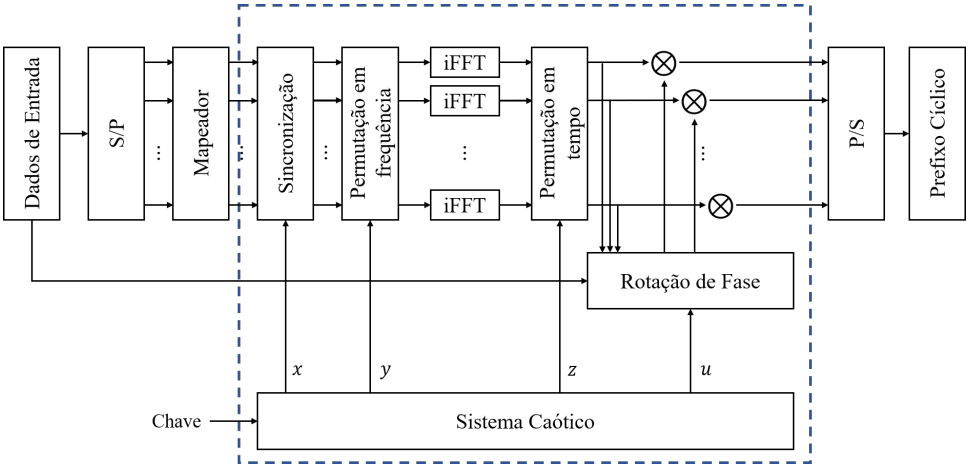


Figura 10 – Diagrama do algoritmo de encriptação da técnica que utiliza sistema caótico 4D. Fonte: adaptado de (YANG *et al.*, 2016).

em tempo e em frequência geram um espaço de $N_{sub}!$ e $N_{simb}!$, respetivamente. Além disso, a rotação de fase tem um espaço de chave proveniente da sensibilidade das condições iniciais, que é igual à 10^{15}. Por fim, a sincronização de tempo dos símbolos OFDM faz com que o espaço de chaves seja 9 vezes maior. Portanto, o espaço de chave total da técnica é $\approx N_{sub}! \times N_{simb}! \times 10^{16}$. Em (YANG *et al.*, 2016), foram utilizadas 64 subportadoras e 64 símbolos, o que gera um espaço de chaves de $\approx 10^{178}$. Assim, robustez dessa técnica à ataques de força bruta é cerca de 10^{100} vezes maior que a do AES-256.

A segunda técnica discutida nesse trabalho utiliza um sistema hipercaótico tridimensional. Proposta em (SULTAN *et al.*, 2018), essa técnica consiste no embaralhamento dos símbolos de sinais 16-QAM OFDM com taxa de 9,4 Gbps a partir de sequências caóticas. Os sinais encriptados foram transmitidos por enlaces de 20 km de fibra óptica. O sistema caótico utilizado pela técnica é dado por

$$\begin{cases} \dot{x} = t_1(y - x) + yz \\ \dot{y} = t_3 x - xz - y \\ \dot{z} = xy - t_2 z \end{cases}, \tag{10}$$

em que t_1, t_2 e t_3 são constantes. As sequências caóticas x, y e z geradas pela solução das equações do sistema são utilizadas para encriptar os sinais.

A Fig. 11 mostra o diagrama de blocos da técnica. Inicialmente, o sistema caótico é solucionado para o conjunto de condições iniciais (chave criptográfica), dando origem às sequências caóticas. A sequência x é convertida em uma sequência binária e passa por uma XOR com o conjunto de bits de entrada. Em seguida, o produto dessa XOR é

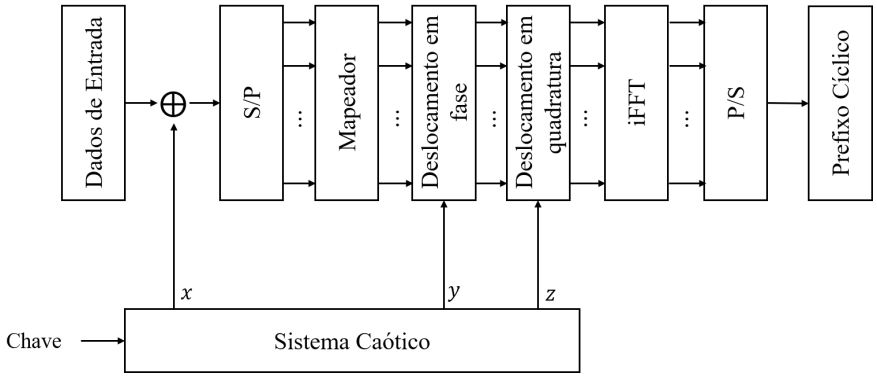


Figura 11 – Diagrama do algoritmo de encriptação da técnica que utiliza sistema caótico 3D. Fonte: adaptado de (SULTAN *et al.*, 2018).

paralelizado e mapeado em um sinal 16-QAM. As sequências y e z são utilizadas para realizar o deslocamento em fase e em quadratura dos símbolos do sinal. Depois desse processo, o sinal passa por uma iFFT, é serializado e o prefixo cíclico é adicionado.

Considerando que a posição inicial dos símbolos da constelação 16-QAM é dada por p, a posição dos símbolos encriptados, P', é dada por

$$P' = (Re[p] \pm \Delta I) + (Im[p] \pm \Delta Q), \tag{11}$$

em que ΔI e ΔQ são dois parâmetros de deslocamento caótico. Esses parâmetros são calculados a partir das sequências caóticas y e z em acordo com

$$\begin{aligned} \Delta I &= y \mod floor(y-1) \\ \Delta Q &= z \mod floor(z-1) \end{aligned} \tag{12}$$

em que a função $floor(\nu)$ arredonda os elementos de ν para os números inteiros mais próximos.

Considerando que são utilizadas N_{sub} subportadoras para sinais 16-QAM e que cada subportadora é representada por 4 bits, o espaço de chaves criado pela operação XOR é de $2^{4\times N_{sub}}$. Para um deslocamento de símbolos considerável na constelação do sinal encriptado, é sugerido uma precisão de 10^{-4} de deslocamento em fase e em quadratura. Dessa maneira, o espaço de chave das operações de deslocamento é de $10^4 \times 10^4$. Portanto, o espaço de chave total da técnica é de $\approx 2^{4\times N_{sub}} \times 10^4 \times 10^4$. Foram utilizadas 128 subportadoras em (SULTAN *et al.*, 2018), o que resulta em um espaço de chaves de $\approx 10^{162}$, um número 10^{85} vezes maior que o do espaço de chaves do AES-256.

Embora as técnicas de criptografia caótica tenham espaços de chave consideravelmente maiores do que o AES, a chave criptográfica deve ser calculada novamente à cada sinal. Essa característica faz com que a técnica seja robusta contra CPAs. Por outro lado, calcular uma nova chave a cada sinal implica em revolver o sistema caótico sempre que um novo sinal for transmitido. Esse pode ser um ponto negativo no ponto de vista do tempo de processamento.

3.4 Criptografia por Fatiamento Espectral

A abordagem de criptografia de sinais baseada em fatiamento espectral consiste em dividir o sinal no domínio da frequência em fatias espectrais, definidas como conjuntos de amostras espectrais, e realizar operações de criptografia. A criptografia de sinais por fatiamento espectral foi proposta, inicialmente, para sinais modulados em frequências ópticas, com as técnicas de codificação espectral por fase (*spectral phase encoding*, SPE) (CORNEJO; PEREZ *et al.*, 2007), codificação espectral por fase e atraso (*spectral phase and delay encoding*, SPDE) (ABBADE *et al.*, 2014; ABBADE *et al.*, 2015; ABBADE *et al.*, 2017) e embaralhamento espectral intercanal (*Shuffling*) (ABBADE *et al.*, 2018; SANTOS *et al.*, 2019).

A implementação das operações de encriptação em sinais ópticos é bastante complexa devido a, principalmente, as não linearidades de componentes ópticos e a quantidade de dispositivos ópticos necessários para fazer realizar operações simples. Seria, por exemplo, inviável realizar operações de criptografia repetidas vezes como as que são consideradas nesse trabalho. Para contornar a dificuldade de realizar operações de criptografia no domínio óptico, é possível implementar técnicas de criptografia por fatiamento espectral em banda base por meio de DSP. Nesse contexto, as técnicas SPE, SPDE e *shuffling* foram propostas por meio de DSP, além da técnica de embaralhamento espectral intracanal (*Scrambling*) (ABBADE *et al.*, 2018; ABBADE *et al.*, 2019; SOUZA *et al.*, 2020; SANTOS, 2020).

Além de contornar as dificuldades inerentes à criptografia no domínio óptico, realizar a criptografia por meio de DSP facilita a combinação e utilização em conjunto de diferentes técnicas de criptografia por fatiamento espectral. As implementação em software por meio

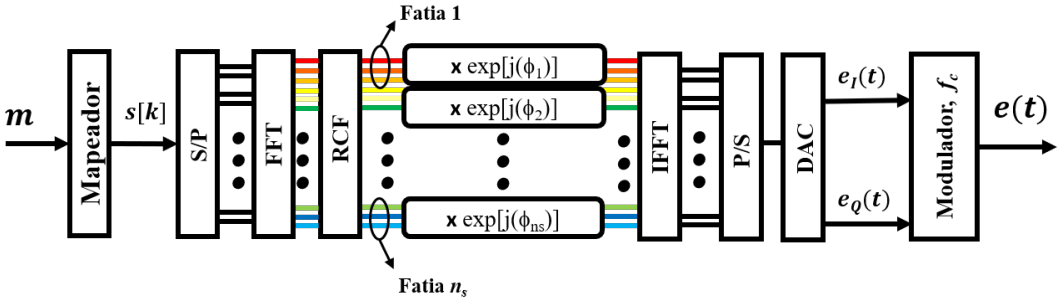


Figura 12 – Diagrama de encriptação da Codificação Espectral por Fase (SPE).

de DSP das técnicas SPE, SPDE, *Scrambling* e *Shuffling* será discutida nas sub-seções seguintes.

3.4.1 Codificação Espectral por Fase (SPE)

A SPE é uma técnica de criptografia de sinais por fatiamento espectal que rotaciona as fases das fatias do sinal em acordo com uma chave. Um diagrama de blocos para a encriptação de sinais pela técnica SPE é apresentado na Fig. 12. A mensagem de entrada, m, é mapeada em um sinal $s[k]$. O sinal é paralelizado por um conversor série-paralelo (S/P), passa por uma transformada rápida de Fourier (*fast Fourier transform*, FFT) e por um filtro cosseno-levantado (*raised-cosine filter*, RCF). O sinal é dividido em n_s fatias e, em seguida, ocorre a operação de encriptação. No processo de encriptação, são adicionadas fases ϕ_i ($i = 1, 2, ..., n_s$) às fases de cada fatia do sinal. As fases são adicionadas multiplicando as fatias por $e^{j\phi_i}$, em que i representa a i-ésima fatia. Após a operação de encriptação, o sinal passa por uma iFFT, é serializado por um conversor parelelo-série (P/S), convertido em um sinal analógico complexo por um conversor digital-analógico (*digital-to-analog converter*, DAC) com compenentes $e_I(t)$ e $e_Q(t)$ e por fim, modula uma portadora, com frequência f_c, originando o sinal encriptado modulado $e(t)$.

A chave criptográfica da técnica SPE é o conjunto de fases ϕ_i adicionadas ao sinal e podem variar entre 0 e 2π. Um receptor autorizado deve adicionar as fases complementares as que foram adicionados na encriptação para recuperar corretamente o sinal.

A BER de sinais encriptados pela SPE é igual a 0,5, o que indica que os sinais são criptografados de maneira satisfatória. Por outro lado, a técnica não confere as propriedades de difusão e confusão aos sinais encriptados. A influência de uma fatia do sinal de entrada não é espalhada para várias fatias do sinal encriptado, ou seja, não tem difusão. Da mesma

maneira, cada fase da chave influencia apenas a fatia do sinal daquela posição, ou seja, a propriedade de confusão não é atendida. Também é possível observar que se o mesmo sinal for encriptado duas vezes com a mesma chave, os sinais encriptados serão iguais. Logo, a técnica também não é robusta contra CPAs.

O número de ataques de força bruta para quebrar a segurança da técnica depende de quanto um invasor pode errar nas fases da chave criptográfica para recuperar corretamente o sinal. Para que um invasor consiga recuperar as informações do sinal corretamente, assume-se que ele deve ter um sinal com a BER no limite da FEC (*forward error correction*) (WANG; SKLAR; JOHNSON, 2001). Na SPE o número de ataques por força bruta necessários é calculado (SANTOS, 2020) em acordo com

$$N_{ataques} = \left(\frac{360}{\Delta\theta}\right)^{n_s} \tag{13}$$

em que n_s é o número de fatias espectrais do sinal e $\Delta\theta$ é o desvio de fase que o invasor pode errar e ainda recuperar o sinal com a BER no limite da FEC.

A SPE multiplica as fatias do sinal por $e^{j\phi_i}$ para adicionar fases às fases do sinal de entrada. Se um invasor utilizar uma sequência de bits com determinada repetição para geral um sinal (100100100, por exemplo), é possível verificar um padrão no sinal encriptado pois diversas componentes espectrais vão receber a mesma fase. Dessa forma, esse invasor pode descobrir a chave. Para contornar esse problema, foi criada a SPDE, que será discutida na próxima sub-seção.

3.4.2 Codificação Espectral por Fase e Atraso (SPDE)

A técnica SPDE, além de ser muito similar à SPE, foi criada para aumentar a segurança dessa. Um diagrama de blocos do processo de encriptação da SPDE é mostrado na Fig. 13. A única diferença é que além de fases, são adicionados atrasos às fatias do sinal. A chave criptográfica da técnica é o conjunto de fases ϕ_i (i = 1, 2, ..., n_s) e atrasos τ_i (i = 1, 2, ..., n_s) utilizadas. Na SPDE, as fatias do sinal de entrada são multiplicadas por $e^{j\phi_i - 2\pi f\tau_i}$.

A técnica SPDE foi proposta, inicialmente, no domínio óptico. Nessa abordagem, cada fatia espectral corresponde a um conjunto de componentes espectrais. A SPDE multiplica as fatias do sinal de entrada por $e^{j\phi_i - 2\pi f\tau_i}$ para adicionar fases e atrasos ao sinal.

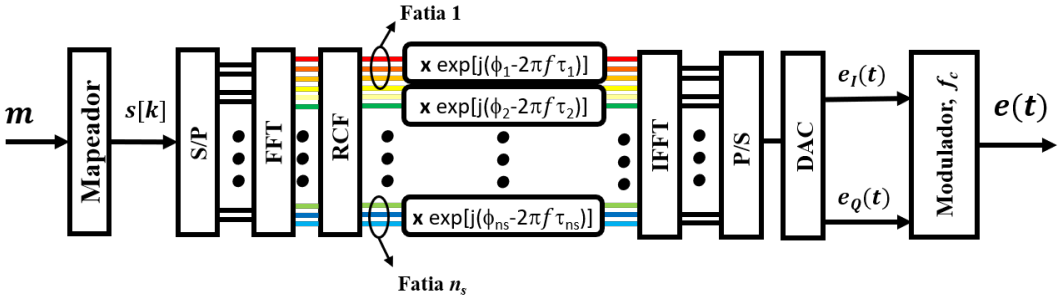


Figura 13 – Diagrama de encriptação da Codificação Espectral por Fase e Atraso (SPDE).

Ao adicionar, além de fases, um atraso às fatias, o atraso de cada componente espectral dentro da fatia dependerá da frequência da componente espectral. Dessa maneira, mesmo que todas as componentes espectrais de uma fatia recebam a mesma fase, os atrasos aplicados a cada componente espectral será diferente e não será possível encontrar um padrão no sinal criptografado (ABBADE *et al.*, 2013).

Ao implementar as técnicas SPE e SPDE por meio de DSP, é possível fazer com que as fatias espectrais sejam compostas por apenas uma amostra espectral. A utilização de uma única amostra por fatia implica que, em uma fatia, não exista amostras em diferentes frequências. Dessa forma, cada amostra receberá uma fase diferente e aplicar atrasos às fatias seria o equivalente à adicionar apenas uma fase. Portanto, em DSP, não é necessário utilizar o atraso e é possível utilizar apenas a SPE sem criar padrões nos sinais criptografados a partir de sinais de entrada provenientes de sequencias repetitivas de bits. A avaliação da segurança com relação as propriedades de difusão e confusão não foram avaliadas na literatura da SPDE, mas a similaridade dessa técnica com a SPE indica que a SPDE também não provê difusão, confusão e robustez contra CPAs.

3.4.3 Embaralhamento Espectral Intracanal (*Scrambling*)

A técnica de embaralhamento espectral intracanal (*Scrambling*) encripta sinais em banda base operando um embaralhamento entre as fatias do sinal. Ou seja, de acordo com uma chave, as fatias trocam de posição. Um receptor autorizado, em posse da chave criptográfica, é capaz de desembaralhar corretamente as fatias do sinal.

O diagrama da técnica *Scrambling* é mostrado na Fig. 14. A mensagem, m, é mapeada no sinal $s[k]$. O sinal s, antes de ser encriptado, é paralelizado, passa por uma FFT e por um filtro RCF. No embaralhador intracanal, as fatias do sinal trocam de posição

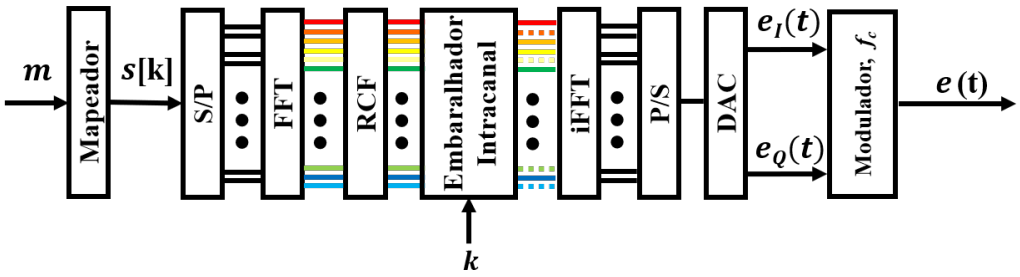


Figura 14 – Diagrama do algoritmo de encriptação do embaralhamento espectral intracanal.

em acordo com uma chave criptográfica, k. Após ser encriptado, o sinal passa por uma iFFT, é serializado, passa por um DAC e então pode ser modulado e transmitido.

Embora seja realizado um embaralhamento entre as fatias do sinal, a influência de uma amostra do sinal de entrada recai apenas sobre a mesma amostra no sinal encriptado. Dessa maneira, a técnica não provê difusão aos sinais encriptados. A influência da chave também não é espalhada, então a técnica não provê confusão aos sinais encriptados. Por fim, dois sinais encriptados com a mesma chave geram os mesmos sinais encriptados, portanto, a técnica não é robusta contra CPAs.

A técnica de *Scrambling* tem um espaço de chaves igual à $n_s!$, em que n_s é o número de fatias espectrais. Seriam necessárias aproximadamente 57 fatias espectrais para que a segurança contra ataques de força bruta do *Scrambling* fosse equivalente à do AES-256 . De fato, o número de fatias utilizado em trabalhos que utilizam criptografia por fatiamento espectral normalmente é bem maior que esse valor.

Em (SANTOS, 2020) é proposta uma técnica que combina o *Scrambling* e a SPE discutida na Subseção 3.4.1. Além disso, são utilizadas chaves dinâmicas (NGO *et al.*, 2010) para prover as propriedades de difusão e confusão aos sinais encriptados. Na abordagem de chaves dinâmicas, as chaves de todos os blocos são calculadas a partir de uma chave inicial. Como cada bloco tem uma chave diferente, a influência das amostras do sinal de entrada e da chave são espalhadas para várias amostras do sinal criptografado. A utilização de chaves diferentes em cada bloco resulta na aleatorização dos sinais encriptados, logo, o *Scrambling* torna-se robusto contra CPAs se utilizado em conjunto com as chaves dinâmicas.

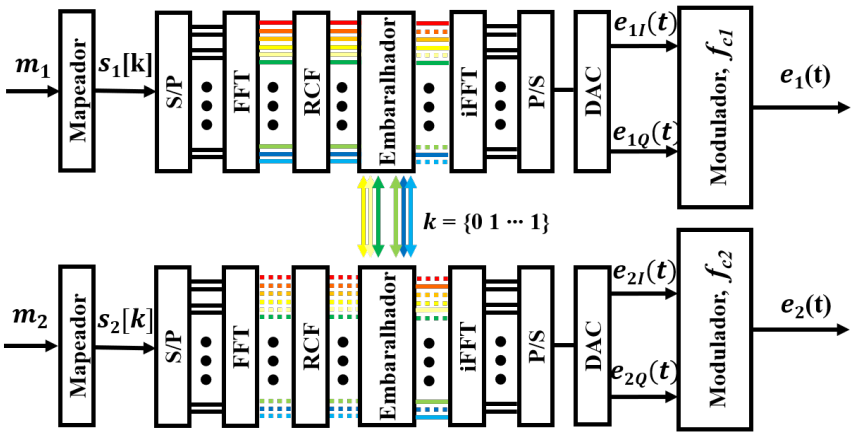


Figura 15 – Diagrama do algoritmo de encriptação do embaralhamento espectral intercanal.

3.4.4 Embaralhamento Espectral Intercanal (*Shuffling*)

A técnica de embaralhamento espectral intercanal (*Shuffling*) (ABBADE *et al.*, 2019) consiste em embaralhar amostras espectrais de sinais diferentes. Os sinais são transmitidos, sendo que podem ser transmitidos por canais em rotas diferentes, e os receptores autorizados, em posse da chave criptográfica, desembaralham os sinais.

A Fig. 15 mostra o diagrama de blocos da técnica. As mensagens, m_1 e m_2, são mapeadas nos sinais $s_1[k]$ e $s_2[k]$. Esses sinais são paralelizados e passam por uma FFT. Os sinais, agora no domínio da frequência, passam por um filtro RCF para serem limitados em banda. Em seguida, as amostras dos sinais são embaralhadas de acordo com uma chave binária k. O embaralhamento funciona da seguinte maneira, se na posição de determinada amostra dos sinals o bit da chave for igual a 1, as amostras são trocadas entre os sinais, e se o bit da chave for igual a 0, nenhuma operação é realizada. Após o embaralhamento, os sinais passam pela FFT, são serializados e passam pelo conversor digital-analógico (*digital-to-analog converter*, DAC). Por fim, os sinais modulam portadoras, f_{c1} e f_{c2}, e são transmitidos.

A principal vantagem com relação à segurança da criptografia por embaralhamento espectral é que para um interceptador ter acesso a um dos sinais, deve monitorar simultaneamente pelo menos dois cabos ópticos da rede para ter acesso aos dois sinais embaralhados. Com relação às propriedades de Shannon, o embaralhamento espectral não confere difusão e confusão aos sinais encriptados. Da mesma maneira que ocorre com a SPE e a SPDE, cada fatia do sinal de entrada influencia apenas na posição em que ela está e a cada componente da chave também não tem a influência espalhada para várias fatias do sinal

encriptado. Além disso, o embaralhamento espectral também não é robusto contra CPAs. Em (SOUZA *et al.*, 2020), foi proposta uma estratégia que combina o Embaralhamento Espectral com a SPE e utiliza o cálculo de chaves dinâmicas (NGO *et al.*, 2010), de maneira que cada bloco usa uma chave diferente e assim, as propriedades de difusão e confusão são atendidas. A utilização de chaves dinâmicas torna aleatórios os sinais encriptados, portanto, a técnica é robusta contra CPAs.

Concluindo o Capítulo 3, observa-se que a criptografia de sinais conta com diversas técnicas em estudo para prover confidencialidade na camada física do modelo OSI. Foram discutidas nesse capítulo técnicas que utilizam diferentes abordagens para criptografar sinais. A criptografia quântica, embora não seja viável para aplicação na transmissão de informações nos sistemas atuais de comunicação devido às baixas taxas de transmissão, é extremamente segura e útil para realizar a troca de chaves criptográficas utilizadas por outras técnicas de criptografia que suportam altas taxas de transmissão. A criptografia caótica tem um alto nível de segurança, alcançando números de ataques por força bruta até 10^{100} vezes maior que os do AES-256. As técnicas de criptografia que utilizam fatiamento espectral tem números de ataques por força bruta maiores que os do AES e como o número de ataques é proporcional ao número de fatias utilizado, a técnica pode ter uma robustez muito grande a esses ataques.

Em algumas abordagens da criptografia de sinais é possível atender as propriedades de difusão e confusão. Mas, no melhor de nosso conhecimento, embora algumas técnicas apresentadas sejam robustas contra CPAs quando utilizam algoritmos de chaves dinâmicas, nenhuma técnica de criptografia de sinais robusta contra CPAs foi proposta. No próximo capítulo será apresentada a estratégia proposta por nosso trabalho.

4 Estratégia proposta

Nesse capítulo serão apresentados os detalhes do desenvolvimento da nova técnica de criptografia de sinais por fatiamento espectral proposta, denominada s-AES. Como discutido anteriormente, objetiva-se utilizar o s-AES em conjunto com um modo de operação desenvolvido para o domínio de sinais, denominado s-CTR. O s-AES e o s-CTR foram desenvolvidos a partir da adaptação de estruturas de criptografia estabelecidas em criptografia de dados, que são, respectivamente, o padrão de criptografia AES e o modo de operação CTR.

A implementação em *software* da nova estratégia de criptografia de sinais é baseada em algoritmos de DSP, em que sinais amostrados são caracterizados, no domínio da frequência, por uma amplitude e por uma fase. Dessa forma, as operações criptográficas são realizadas nas amplitudes e fases das amostras dos sinais. As Seções 4.1 e 4.2 abordam em detalhes o desenvolvimento do s-AES e do s-CTR, respectivamente.

4.1 s-AES

A relação entre o padrão AES e o s-AES é mostrada no diagrama de blocos da Fig. 16. A Fig. 16 (a) mostra o diagrama de blocos do AES e a Fig. 16 (b) mostra o diagrama de blocos do s-AES. No padrão AES, blocos de dados com comprimento de 128 bits são processados pelas operações criptográficas descritas no Capítulo 2. Já no s-AES, blocos de dados são mapeados em 125 símbolos. Esse sinal, com taxa de amostragem de 2 amostras/símbolo, é transformado para o domínio da frequência por meio de uma FFT. Em seguida, o sinal é limitado em banda por um RCF com fator de *roll-off* de 2,4%. Após o RCF, temos um sinal com 128 amostras espectrais não nulas. É importante destacar que o valor do fator de *roll-off* foi escolhido para que as operações criptográficas adaptadas para o domínio de sinais atuem sobre conjuntos de informação com o mesmo comprimento dos blocos de dados do AES.

No espectro do sinal limitado em banda pelo RCF existem algumas componentes espectrais com amplitudes menores que a amplitude média do sinal na região do *roll-off*. Um interceptador, com acesso ao sinal criptografado, pode tentar descobrir o conteúdo do sinal por meio das amostras do sinal. Amostras com maiores amplitudes tem mais energia e,

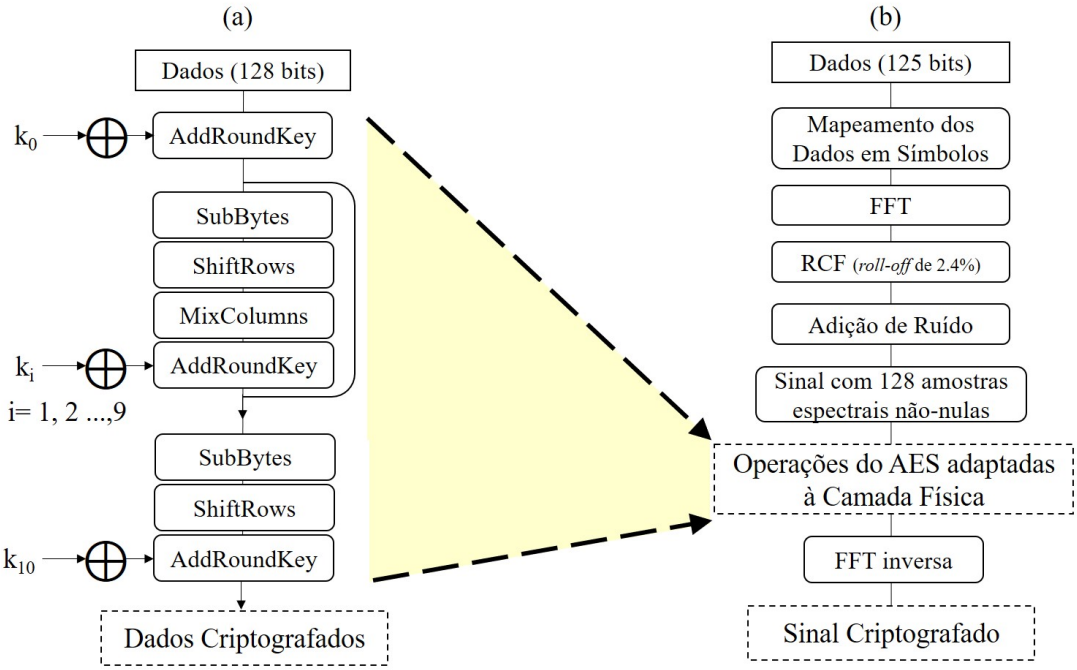


Figura 16 – Diagrama de blocos da adaptação do padrão AES para o s-AES.

consequentemente, mais informações. Dessa maneira, em um ataque, o interceptador pode descartar amostras com menores amplitudes e recuperar o sinal com um erro aceitável. Para evitar que o interceptador possa descartar as amostras da região de *roll-off*, uma estratégia possível é forçar que todas as componentes espectrais tenham, aproximadamente, a mesma amplitude. Seguindo essa estratégia, optamos por adicionar um ruído ao sinal para que esse seja branco em toda a banda. O sinal branco passa por operações do AES adaptadas à camada física. O sinal criptografado passa então, por uma iFFT e pode ser transmitido.

A adaptação das operações do AES para a camada física requer a definição de algumas analogias entre o AES e o s-AES. São elas:

1. A unidade de informação do AES é o bit, enquanto a unidade de informação análoga no s-AES é a fase de cada amostra do sinal;
2. No AES, um byte é o conjunto de 8 bits. Analogamente, no s-AES, um s-byte é definido como um conjunto de fases de 8 amostras;
3. Cada bloco do AES é composto por 16 bytes. No s-AES, cada s-bloco é composto por 16 s-bytes; Os 16 s-bytes do s-AES são organizados em matrizes de 4x4 s-bytes, análogas às matrizes de 4x4 bytes do AES.

4. As chaves utilizadas no AES tem comprimento de 128 bits. Analogamente, cada s-shave é composta de 128 fases.

Além das analogias definidas, foi elaborada uma função que realiza o mapeamento de fases em valores binários (0's e 1's). Esse mapeamento é utilizado para viabilizar a execução de determinadas funções criptográficas do AES que serão detalhadas posteriormente. O mapeamento de fases pode ser realizado em diversos níveis, não apenas em valores binários. Em nosso trabalho optou-se por utilizar o mapeamento binário para manter uma analogia direta com o AES e verificar se dois níveis são suficientes para prover boa robustez contra ataques. O mapeamento em mais níveis requer uma redefinição das tabelas de substituição e matrizes de multiplicação utilizadas no AES. Esse processo não faz parte do escopo desse trabalho e é um tópico interessante para trabalhos futuros. O mapeamento utilizado nesse trabalho é realizado em acordo com:

$$F(\varphi_{\text{in}}) = \begin{cases} 0 & \text{se} \quad 0 \leq \varphi_{\text{in}} < \pi \\ 1 & \text{se} \quad \pi \leq \varphi_{\text{in}} < 2\pi \end{cases}, \tag{14}$$

em que φ_{in} é a fase de entrada da função.

Uma vez que as analogias entre o AES e o s-AES e a função de mapeamento foram definidas, as funções utilizadas pelo AES foram adaptadas para o domínio de sinais. Além das operações criptográficas utilizadas nos *rounds* do AES, também foi necessário adaptar a expansão de chaves para processar s-chaves compostas de fases.

Na expansão de chaves do AES, a chave k_i é calculada a partir de k_{i-1}. Na adaptação da expansão de chaves desenvolvida para o s-AES, o cálculo da s-chave k_i é realizado da seguinte maneira: as 128 fases da s-chave k_{i-1} são mapeadas em bits em acordo com F, os 128 bits provenientes do mapeamento passam pelas operações definidas na expansão de chaves do AES, os bits resultantes dessas operações são mapeados em fases 0 ou π e adicionados às fases da s-chave k_{i-1}.

As operações criptográficas AddRoundKey, SubBytes, ShiftRows e MixColumns foram adaptadas para o domínio de sinais e serão denominadas s-AddRoundKey, s-SubBytes, s-ShiftRows e s-MixColumns. As subseções a seguir detalham o funcionamento da primeira versão dessas operações.

4.1.1 s-AddRoundKey

A operação AddRoundKey do AES realiza uma XOR entre os bits do bloco de entrada da operação com a chave k_{i}. Enquanto no AES as unidades de informação são os bits 0's e 1's, as unidades de informação do s-AES são fases que podem assumir quaisquer valores no intervalo $[0, 2\pi)$. Dessa maneira, foi necessário definir uma operação análoga ao XOR para o s-AddRoundKey, o s-XOR.

O s-XOR deve operar as fases do sinal de entrada da operação e as fases da s-chave. A saída do s-XOR deve ser uma fase no intervalo $[0, 2\pi)$, assim como é o intervalo das fases de entrada da operação. Nesse trabalho, o s-XOR realiza uma soma em módulo 2π entre as fases das amostras do bloco de entrada com as fases da s-chave k_{i} em acordo com

$$\theta_{out}(\mathrm{j}) = (\theta_{in}(\mathrm{j}) + \theta_{k_{\mathrm{i}}}(\mathrm{j})) \mod 2\pi, \tag{15}$$

em que $\theta_{out}(\mathrm{j})$ é a fase da j-ésima amostra do sinal de saída da operação AddRoundKey, $\theta_{in}(\mathrm{j})$ é a fase da j-ésima amostra do sinal de entrada e $\theta_{k_{\mathrm{i}}}(\mathrm{j})$ é a j-ésima fase da s-chave k_{i}. A soma da fase da chave na fase do sinal ocasiona um deslocamento da fase do sinal, similar à técnica SPE discutida no Capítulo 3.

4.1.2 s-SubBytes

Existem diversas possibilidades para a definição operação s-SubBytes. No AES, as tabelas de substituição são determinadas a partir de funções que minimizam a eficiência de ataques diferenciais. O funcionamento de ataques diferenciais e a definição de estratégias para minimizá-los no domínio de sinais está em investigação e compõem os tópicos para trabalhos futuros. Na adaptação da operação SubBytes para a operação s-SubBytes por meio da analogia com o AES, a função de mapeamento de fases é utilizada. Os 16 s-bytes de entrada são mapeados em 16 bytes por meio da função de mapeamento e passam pela operação SubBytes da mesma maneira que é realizada no AES. Em seguida, os bytes resultantes da operação SubBytes são mapeados em s-Bytes. Por fim, as fases que compõem os 16 s-bytes resultantes da operação são adicionadas às fases do sinal de entrada da operação.

Por exemplo, considerando que o i-ésimo s-byte é igual a s-B_i= {0,2π; 0,5π; 0,3π; 1,2π; 1,5π; 0,4π; 0,7π; 1,7π}. O mapeamento em byte, em acordo com (14), será B_i = $\{F(0,2\pi); F(0,5\pi); F(0,3\pi); F(1,2\pi); F(1,5\pi); F(0,5\pi); F(0,7\pi); F(1,7\pi)\}$ = {0; 0; 0; 1; 1; 0; 0; 1}. O byte B_i passa pela operação SubBytes e é substituído pelo byte Bs_i = {1; 1; 0; 1; 0; 1; 0; 0}. Esse byte é convertido para um s-Byte e somado a s-B_i, ou seja, a saída da operação s-SubBytes será s-B_i + {π; π; 0; π; 0; π; 0; 0} = {1,2π; 1,5π; 0,3π; 0,2π; 1,5π; 1,4π; 0,7π; 1,7π}.

4.1.3 s-ShiftRows

O ShiftRows utilizado no AES realiza deslocamentos de bytes das linhas da matriz 4x4 bytes e não depende de funções algébricas. Dessa maneira, a adaptação para o s-ShiftRows é direta. Assim como no ShiftRows, o deslocamento dos s-bytes no s-ShiftRows segue as seguintes regras:

- Nenhum s-byte da primeira linha é deslocado;
- Um s-byte da segunda linha é deslocado;
- Dois s-bytes da terceira linha são deslocados;
- Três s-bytes da quarta linha são deslocados.

4.1.4 s-MixColumns

A operação MixColumns do AES realiza a multiplicação entre as colunas da matriz de 4x4 bytes e uma matriz conhecida. Para adaptar a MixColumns para a s-MixColumns foi utilizada a função de mapeamento de fases.

De maneira similar ao que ocorre na operação s-SubBytes, os s-bytes do sinal de entrada da s-MixColumns são mapeados em bytes, passam pela operação MixColumns definida no AES e os bytes resultantes dessa operação são convertidos em s-bytes. Por fim, os s-bytes da saída da s-MixColumns são somados aos s-bytes da entrada.

Nesse ponto, é importante mencionar que o resultado para a propagação de sinais encriptados pela primeira versão do s-AES, descrita acima, mostrou que a técnica agrega penalidades que inviabilizam a sua utilização da maneira que está definida. Observa-se que

a primeira versão das operações s-SubBytes e s-MixColumns realiza o mapeamento das fases do sinal de entrada da operação. Quando o sinal é encriptado e transmitido por um canal com ruído aditivo Gaussiano branco (*additive white Gaussian noise*, AWGN), o ruído altera a fase das amostras do sinal e o mapeamento pode ser comprometido no processo de desencriptação. Por exemplo, supondo que determinada amostra de um sinal que não passou por nenhuma operação de criptografia tem fase igual a $0{,}9\pi$ e que após o processo de criptografia, a fase dessa amostra é igual a $1{,}9\pi$. Se essa amostra for transmitida por um canal que não agrega nenhuma penalidade, no processo de desencriptação, determinada operação que utiliza o mapeamento de fase a converterá para 1 e conseguirá recuperar a fase corretamente. Agora, se o sinal for transmitido por um canal AWGN, a fase da amostra na entrada do receptor é diferente da que foi transmitida e pode ser, por exemplo, igual a $0{,}3\pi$. Nesse caso, operações que utilizam o mapeamento de fase vão mapear essa fase para 0 e não será possível recuperar a fase do sinal corretamente.

Visando resolver esses problemas foram desenvolvidas duas novas versões das operações s-SubBytes e s-MixColumns. Na segunda versão, as operações foram redefinidas para operar baseadas na s-chave e não dependerem das fases dos sinais de entrada. Na terceira versão, a redefinição da s-SubBytes baseou-se na utilização da s-chave para aplicar uma função não linear às fases do sinal e, na redefinição da s-MixColumns, a s-chave foi utilizada para definir posições de permutação das fases das amostras do sinal. Adiantamos aqui que a segunda versão possibilitou recuperar os sinais em cenários em que sinais criptografados são transmitidos por canais AWGN com penalidade desprezível e a terceira versão, mesmo após testes com diversas funções não lineares, sempre conduziu a penalidades de no mínimo 5 dB.

Apesar da segunda versão das operações s-SubBytes e s-MixColumns ter funcionado sem agregar penalidades, verificamos que uma estratégia mais interessante é manter as operações originais e aplicar um modo de operação que viabilize a utilização da primeira versão das operações sem agregar penalidades. No modo de criptografia CTR, por exemplo, a técnica de encriptação utilizada não atua sob o bloco de informação. Como foi visto no Capítulo 2, a técnica atua sob um vetor β_i, composto por um *nonce* e um *counter*. O bloco de informação passa por uma XOR com vetor γ_i. A adaptação do CTR para o s-CTR, que será discutida na Seção 4.2, segue o mesmo princípio. Portanto, o s-AES não atuará sob as amostras do sinal e dessa maneira, a primeira versão das operações s-SubBytes e s-MixColumns não implicam em penalidades e podem ser utilizadas. De fato, para ser tão

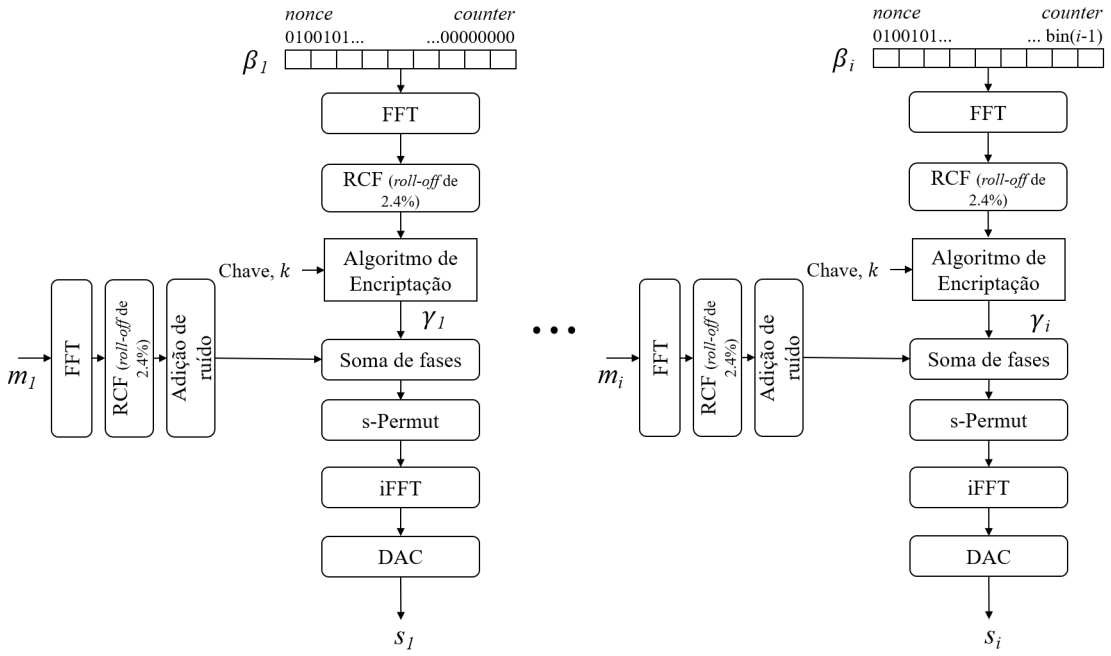


Figura 17 – Diagrama de blocos da adaptação do modo de operação CTR para o s-CTR.

fiel à analogia com o AES quanto possível, a primeira versão dessas operações, definidas em 4.1.2 e 4.1.4, são utilizadas na versão final da proposta que será apresentada no fim desse capítulo.

4.2 s-CTR

O modo de operação CTR foi adaptado para atuar no domínio de sinais, em que foi denominado s-CTR. A Fig. 17 mostra o diagrama de blocos do s-CTR. Na adaptação, o vetor β_i é mapeado em um sinal, passa por uma FFT e é transmitido por um RCF com *roll-off* de 2,4 %. Esse sinal passa por um algoritmo de encriptação, originando o sinal γ_i.

O bloco de mensagem m_i é mapeado em um sinal, passa por uma FFT, é transmitido por um RCF com um *roll-off* de 2,4 % e é adicionado a um ruído para que o sinal seja aproximadamente branco. Enquanto no CTR é realizada uma XOR entre a mensagem e o vetor γ_i, no s-CTR é realizada uma soma de fases, em que as fases das amostras do vetor γ_i são adicionadas às fases do sinal branco. Após esse processo, foi incluída outra operação de criptografia que não é realizada no CTR, denominada s-Permut.

A operação s-Permut realiza uma permutação das amostras do sinal em acordo com a ordenação das fases do vetor γ_i. Por exemplo, supõe-se um bloco na saída da soma de fase é composto por 4 amostras descritas por $\{(A_1; \varphi_1), (A_2; \varphi_2), (A_3;\varphi_3), (A_4;\varphi_4)\}$

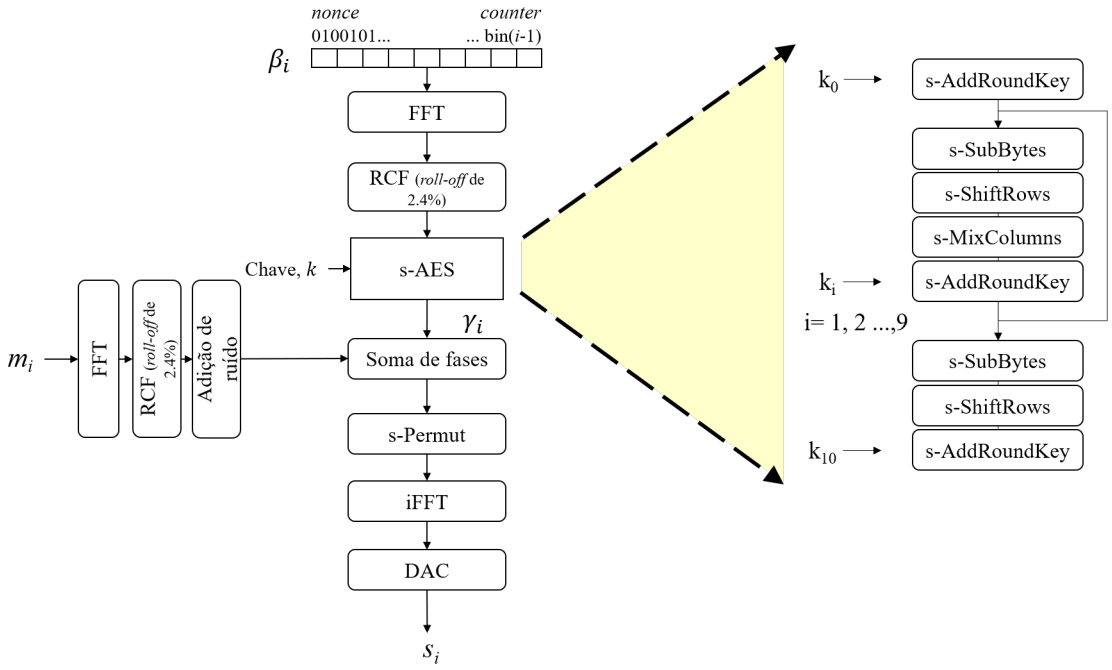


Figura 18 – Diagrama de blocos da estratégia proposta por esse trabalho, o s-AES integrado ao modo de operação CTR.

= {(0,2; 150°), (0,5; 10°), (0,3; 40°), (0,8; 25°)}. Se γ_i = {(0,35; 230°), (0,9; 15°), (0,5; 130°); (0,7; 40°)}, a ordenação das fases leva a $\varphi_2 = 15°$, $\varphi_4 = 40°$, $\varphi_3 = 130°$ e $\varphi_1 = 230°$. Os índices das fases são: 2, 4, 3, 1 e após a operação s-Permut o bloco encriptado é dado por: {(0,5; 10°), (0,8; 25°), (0,3; 40°), (0,2; 150°)}. Após a operação s-Permut, o sinal encriptado passar por uma iFFT, é convertido em um sinal analógio por um DAC e pode ser modulado e transmitido.

Por fim, a estratégia proposta desse trabalho é utilizar a nova técnica de criptografia espectral de sinais, o s-AES, em conjunto com o modo de operação s-CTR. A Fig. 18 mostra o diagrama de blocos do s-AES integrado ao modo de operação s-CTR. Para a compatibilidade com o s-AES, o vetor β_i tem comprimento de 125 bits, sendo 61 bits dedicados para o *nonce* e 64 bits dedicados para o *counter*. Dessa maneira, serão 128 amostras espectrais não nulas após o RCF com *roll-off* de 2,4 %, comprimento compatível com o s-AES.

Nesse capítulo foi apresentada a estratégia proposta por esse trabalho. Observa-se que para chegar em uma proposta final, alguns passos foram necessários. Inicialmente, a primeira versão da adaptação do AES para o s-AES foi desenvolvida por meio de uma analogia direta. Porém, a transmissão de sinais encriptados por essa estratégia foi

inviabilizada devido as penalidades agregadas pela técnica. Foram desenvolvidas então, duas novas versões do s-AES em que as operações s-SubBytes e s-MixColumns foram redefinidas. Embora uma dessas novas versões viabilizasse a transmissão de sinais criptografados, optou-se por utilizar a primeira versão do s-AES e integrá-la ao s-CTR. A estratégia proposta possibilita a utilização primeira versão do s-AES sem comprometer a transmissão de sinais criptografados, além de aleatorizar os sinais encriptados e possibilitar a reutilização de chaves. A análise da técnica, bem como avaliação da transmissão de sinais criptografados pela estratégia proposta e a análise de segurança da técnica, serão discutidas no Capítulo 5.

5 Resultados

Nesse capítulo avaliaremos o desempenho do s-AES integrado ao s-CTR. Denominaremos a integração do s-AES com o modo de operação s-CTR de s-AES/s-CTR a partir dessse ponto do trabalho. Podemos dividir a avaliação do desempenho da técnica em (a) análise do processo de encriptação e desencriptação da técnica, (b) aplicabilidade da transmissão de sinais criptografados por um canal AWGN e por um enlace óptico e (c) segurança da técnica. A descrição das simulações e os resultados obtidos para (a), (b) e (c) são apresentados nas Seções 5.1, 5.2 e 5.3, respectivamente.

5.1 Análise do s-AES/s-CTR

Para avaliar o processo de encriptação, foram avaliados os espectros, constelações e histogramas de amplitude e de fase de sinais de entrada, encriptados e desencriptados. Conforme especificado no Capítulo 4, foram considerados, nas simulações computacionais, blocos de dados com 125 símbolos. Ou seja, blocos de 125 bits para simulações com sinais BPSK, blocos de 250 bits para sinais QPSK e blocos com 500 bits para sinais 16-QAM. O RCF utilizado para limitar a banda dos sinais, também em acordo com o que foi definido

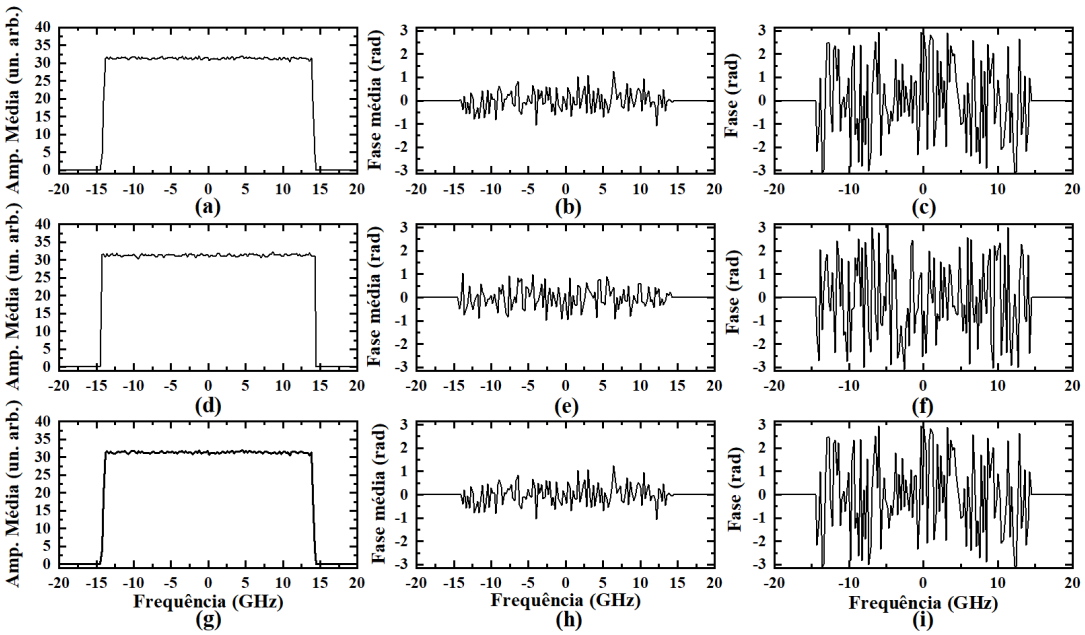


Figura 19 – Espectros de (a) amplitude média, (b) fase média e (c) fase do sinal de entrada; (d) amplitude média, (e) fase média e (f) fase do sinal encriptado; (g) amplitude média, (h) fase média e (i) fase do sinal desencriptado.

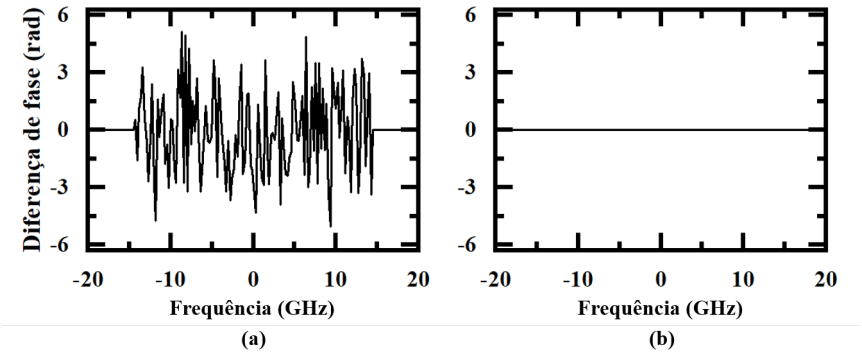


Figura 20 – Diferença de fase (a) entre o espectro de fase do sinal de entrada e do sinal encriptado e (b) entre o espectro de fase do sinal de entrada e do sinal encriptado.

no Capítulo 4, conta com um fator de *roll-off* $r = 2{,}4\%$. Adotamos uma taxa de símbolo de 28 GSamples/s e dessa maneira, os sinais tem banda $B = 14{,}34$ GHz. Para alcançar precisão estatística nos resultados, foram simulados 3000 blocos. Os bits que compõem os blocos correspondem a uma sequência binária pseudo-aleatória (*pseudorandom binary sequence*, PRBS) e foi utilizada uma única s-chave, gerada aleatoriamente, para todos os blocos.

A Fig. 19 mostra os espectros dos sinais 16-QAM de entrada ((a), (b) e (c)), encriptados ((d), (e) e (f)) e desencriptados ((g), (h) e (i)). Os espectros de amplitude ((a), (d) e (g)) mostram a média entre os espectros de amplitude dos 3000 blocos. Para os espectros de fase, são apresentadas tanto as médias entre todos os espectros simulados ((b), (e) e (h)) quanto o espectro de fase de um único sinal ((c), (f) e (i)). Comparando as figuras da primeira linha (sinais de entrada) com as da última linha (sinais desencriptados), é possível observar que a técnica consegue recuperar os sinais pois essas são aproximadamente iguais. Nos espectros de fase do sinal encriptado, Fig. 19 (e) e (f), é possível observar com clareza o efeito da técnica de encriptação pois os valores de fases são consideravelmente diferentes das fases do sinal de entrada.

Para verificar o efeito da criptografia nos espectros de fases dos sinais, a Fig. 20 mostra as diferenças de fases entre o espectro de fases do sinal de entrada e do sinal encriptado e a diferença de fases entre o espectro de fases do sinal de entrada e do sinal desencriptado. A Fig. 20(a) mostra que as fases do sinal encriptado diferem das fases do sinal de entrada entre -2π e 2π. Esse resultado indica que está ocorrendo uma rotação de fase em todas as amostras do sinal de entrada, como era esperado. É possível observar na

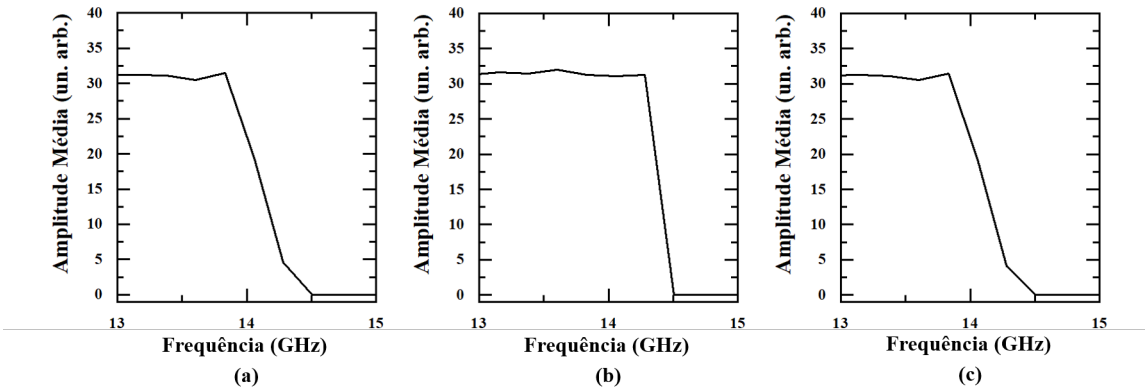


Figura 21 – Espectros de amplitude média do sinal de (a) entrada, (b) encriptado e (c) desencriptado.

Fig. 20(b) que o processo de desencriptação ocorre corretamente e não existe nenhuma diferença de fase entre o sinal desencriptado e o sinal de entrada.

O s-AES/s-CTR adiciona um ruído no sinal de entrada e o torna aproximadamente branco para que interceptadores não sejam capazes de recuperar informações do sinal descartando as amostras de menor potência que estão na região de *roll-off*. É possível observar o efeito da adição de ruído se aproximarmos o gráfico do espectro de amplitudes nessa região. A Fig. 21 mostra os espectros de amplitude média do sinal (a) de entrada, (b) encriptado e (c) desencriptado entre 13 GHz e 15 GHz. Observa-se que no sinal encriptado existe um decaimento com algumas amostras com amplitudes intermediárias na região de *roll-off*, ou seja, entre $B(1-0,024) = 13{,}99$ GHz e $B(1+0,024) = 14{,}68$ GHz. No sinal encriptado, em que foi adicionado um ruído, o decaimento não é observado e o sinal é aproximadamente plano. O sinal é desencriptado corretamente e o ruído é removido, portanto, o sinal desencriptado é igual ao sinal de entrada. A avaliação dos

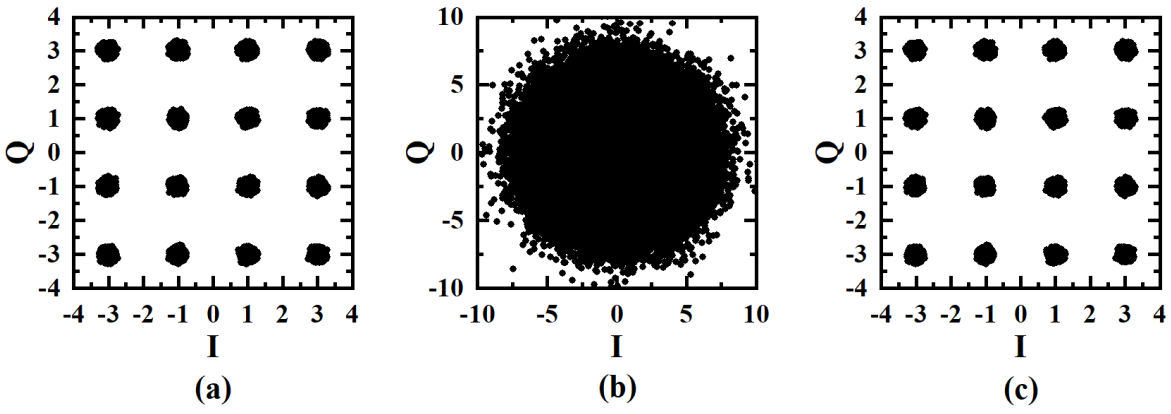


Figura 22 – Constelações dos sinais 16-QAM (a) de entrada, (b) encriptados e (c) desencriptados.

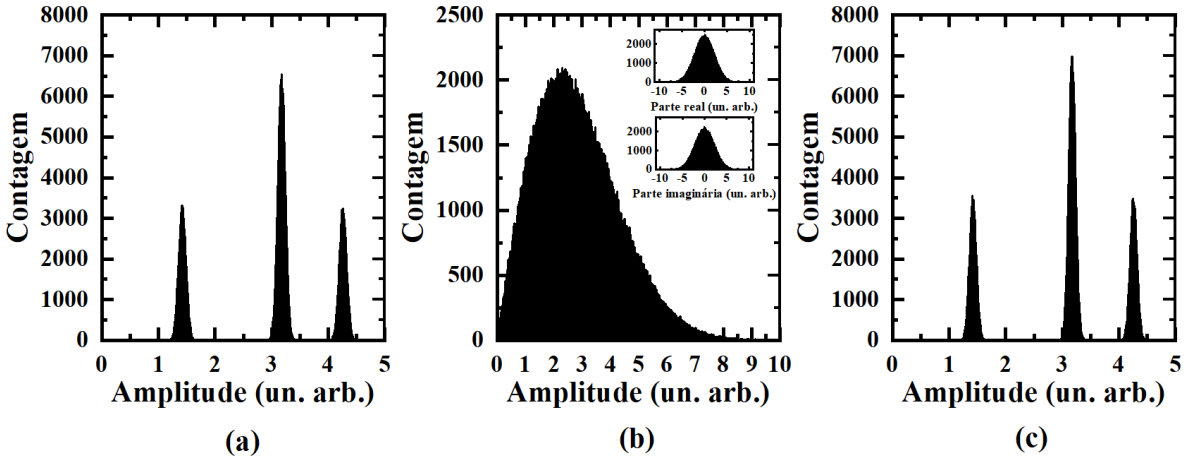


Figura 23 – Histogramas de amplitudes dos sinais 16-QAM (a) de entrada, (b) encriptados e (c) desencriptados.

espectros dos sinais indica que o s-AES/s-CTR encripta e desencripta sinais corretamente. Além da análise dos espectros, as constelações dos sinais foram utilizadas para avaliar o funcionamento da estratégia. A Fig. 22 mostra as constelações dos sinais de entrada, encriptados e desencriptados. As constelações apresentadas são referentes aos 3000 blocos simulados. Na constelação do sinal de entrada, Fig. 22 (a), os 16 símbolos do sinal 16-QAM estão bem definidos. O diâmetro de cada símbolo é ligeiramente maior do que o convencional devido à utilização do RCF e pelo fato de estarmos utilizando apenas 125 símbolos. Caso utilizássemos um número maior de símbolos, esse diâmetro seria reduzido. De fato, constatamos que o diâmetro observado para 125 símbolos praticamente não agrega penalidade e não compromete os resultados obtidos.

Na constelação do sinal encriptado, Fig. 22 (b), observa-se que todos os símbolos simulados distribuem-se por uma mancha circular. Essa constelação sugere que um interceptador encontrará dificuldade para recuperar o sinal. De fato, a BER calculada é de aproximadamente 0,5. A Fig. 22 (c) mostra a constelação do sinal após o processo de desencriptação. Os símbolos voltam a ficar bem definidos e nos mesmos pontos que os símbolos da constelação dos sinais de entrada.

Assim como os espectros dos sinais, as constelações indicam que o s-AES/s-CTR encripta e desencripta sinais corretamente. Para finalizar a análise da técnica, os histogramas de amplitude e fase dos sinais de entrada, encriptados e desencriptados serão avaliados. A Fig. 23 mostra os histogramas de amplitudes dos sinais 16-QAM (a) de entrada, (b) encriptados e (c) desencriptados. O histograma do sinal de entrada possui 3

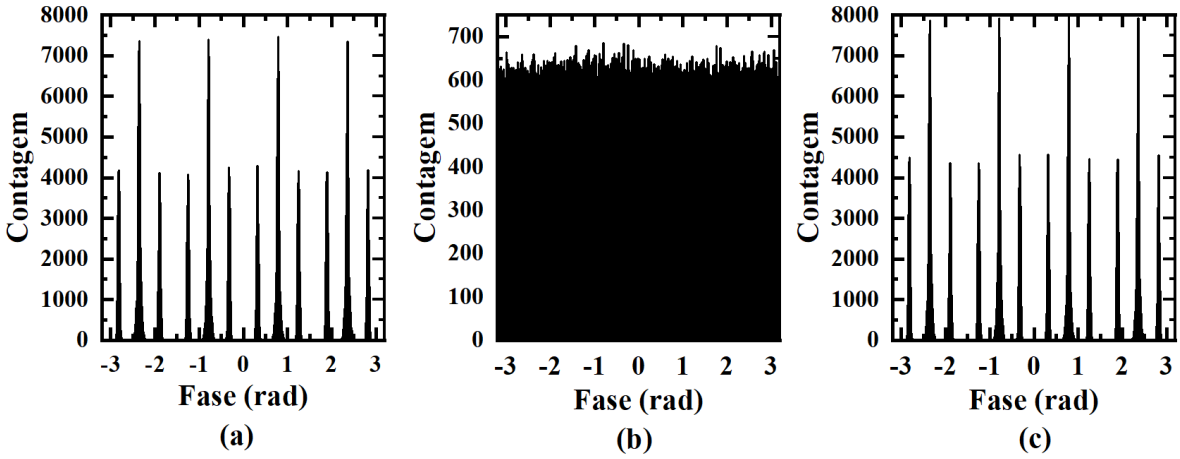


Figura 24 – Histogramas de fases dos sinais 16-QAM (a) de entrada, (b) encriptados e (c) desencriptados.

gaussianas centradas nas amplitudes $\sqrt{2}$, $\sqrt{10}$ e $3\sqrt{2}$. A gaussiana localizada em $\sqrt{10}$ tem aproximadamente o dobro da contagem das outras duas porque temos 4 símbolos com amplitude $\sqrt{2}$, 8 símbolos com amplitude $\sqrt{10}$ e 4 símbolos com amplitude $3\sqrt{2}$. Para verificar esse resultados, observemos a constelação do sinal de entrada, Fig. 22(a). Os 4 símbolos no centro tem amplitude igual a $\sqrt{2}$, os 4 símbolos dos cantos tem amplitude igual a $3\sqrt{2}$ e os 8 demais símbolos tem amplitude igual a $\sqrt{10}$.

O histograma de amplitudes do sinal encriptado, Fig. 23 (b), tem distribuição de Rayleigh, resultado da combinação de dois histogramas com distribuição gaussiana, um no eixo I e outro no eixo Q (Lathi; Ding, 2012). Na constelação do sinal encriptado, Fig. 22(b), a visualização das gaussianas nos eixos I e Q não é muito direta, mas é possível observar que os símbolos ficam mais afastados entre si quanto maior a distância do centro da constelação, o que indica um comportamento gaussiano que é comprovado no histograma. As amplitudes do sinal são recuperadas corretamente e o histograma do sinal desencriptado é aproximadamente igual ao histograma do sinal de entrada.

Os histogramas de fase dos sinais 16-QAM (a) de entrada, (b) encriptados e (c) desencriptados são apresentados na Fig. 24. No histograma de fase dos sinais de entrada, Fig. 24(a), existem símbolos em 12 valores de fase diferentes, sendo que em 4 valores de fase a contagem no histograma é aproximadamente o dobro das outras. De fato, ao observar a constelação do sinal de entrada, Fig. 22(a), existem 4 fases com o dobro de símbolos com relação às outras 8 fases. O histograma de fases do sinal encriptado tem distribuição aproximadamente uniforme pois, como é possível observar na Fig. 22(b), os símbolos do

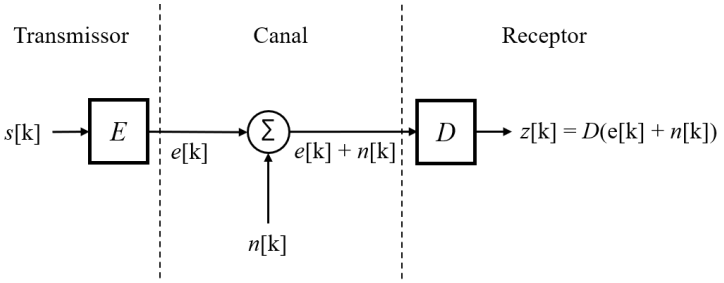


Figura 25 – Diagrama simplificado da transmissão de sinais por um canal AWGN.

sinal estão dispostos uniformemente em todos os valores de fase. De fato, como as fases das amostras do sinal são rotacionadas em acordo com operações que são realizadas a partir de chaves uniformemente geradas, o resultado é uma distribuição uniforme de fases.

Com os resultados discutidos nessa seção, verificou-se que o s-AES/s-CTR é capaz de encriptar e desencriptar sinais corretamente. Um interceptador que consiga ter acesso ao sinal encriptado, não consegue recuperar o sinal de entrada sem efetuar algum tipo de ataque. Caso o interceptador faça uma medida dos espectros do sinal encriptado, o espectro de amplitude medido será o de um sinal branco que está embaralhado e o espectro de fase medido será o de um sinal que teve os valores de fase rotacionados pelo s-AES/s-CTR e também está embaralhado. Se o interceptador tiver acesso à constelação do sinal encriptado, não terá nenhuma informação do sinal além de uma mancha circular em que os pontos bem definidos da constelação do sinal original não existem. Por fim, se o interceptador tentar ter acesso às informações do sinal por meio dos histogramas de amplitude ou fase do sinal, terá acesso apenas a um histograma de amplitudes com uma distribuição de Rayleigh ou a um histograma de fases com distribuição uniforme. Em ambos os casos, não é possível obter informações sobre o sinal sem algum tipo de ataque. Uma vez que foi verificada a capacidade técnica em encriptar e desencriptar sinais, a transmissão de sinais criptografados e a segurança da técnica serão discutidas nas seções a seguir.

5.2 Trasnsmissão de sinais criptografados

Foram simuladas as transmissões de sinais criptografados por um canal AWGN e por um canal óptico. A simulação da transmissão de sinais pelo canal AWGN foi realizada no MATLAB. Nesse cenário, o transmissor é responsável por gerar e encriptar os sinais, o canal adiciona o ruído AWGN aos sinais e por fim, o receptor desencripta os sinais. A Fig. 25 mostra uma versão simplificada do diagrama de blocos do transmissor, canal e receptor

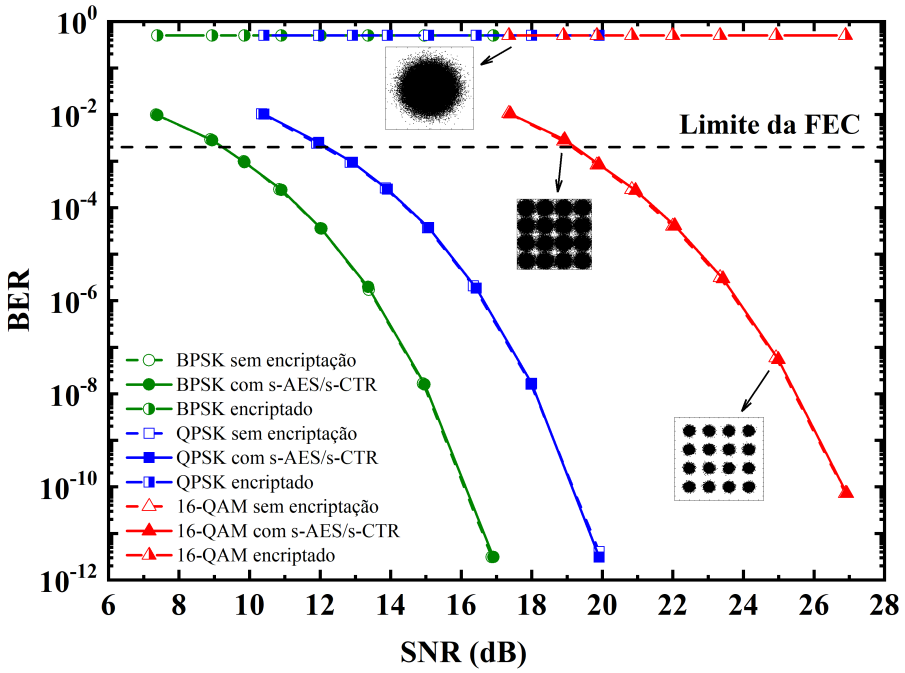


Figura 26 – BER em função da SNR para sinais BPSK, QPSK e 16-QAM transmitidos por um canal AWGN.

em um processo de transmissão de um sinal. Um sinal amostrado s[k] é encriptado pelo algoritmo de encriptação E, gerando o sinal encriptado e[k] O sinal e[k] é transmitido pelo canal AWGN, em que o ruído n[k] é adicionado. No receptor, o algoritmo D desencripta o sinal ruidoso, gerando o sinal z[k]. O sinal desencriptado é o resultado da desencriptação da soma do sinal encriptado com o ruído.

Os parâmetros de simulação utilizados para a transmissão de sinais por um canal AWGN foram os mesmos da análise da técnica, com a exceção de que foi realizada a transmissão de 1000 blocos. Consideraremos, nesse trabalho, que um interceptador é capaz de recuperar o sinal no limite da BER da FEC. O limite da BER adotado nesse trabalho é de 2.10^{-3}, padronizado pela recomendação G.975.1 (2004) do ITU-T (TychopouloS; Koufopaulou; Tomkos, 2006).

A Fig. 26 mostra a BER em função da razão sinal-ruído (*signal-to-noise ratio*, SNR) para a transmissão de sinais BPSK, QPSK e 16-QAM. Os resultados obtidos para a propagação de sinais encriptados e desencriptados pelo s-AES/s-CTR foram comparados com os resultados obtidos para a propagação de sinais de referência, ou seja, sinais que foram transmitidos sem realizar nenhum processo de criptografia. As curvas obtidas mostram que a estratégia proposta não agrega nenhuma penalidade significativa em cenários em

que os sinais criptografados são transmitidos por um canal AWGN. Observa-se que as curvas para o sinais que foram encriptados e desencriptados pelo s-AES estão sobrepostas às curvas de referência.

De fato, esse resultado era esperado pois as operações de encriptação e desencriptação realizadas não devem alterar a SNR dos sinais. A potência do sinal desencriptado é igual a variância desse sinal, calculada por

$$\sigma_z^2 = \sigma_{D(e[\mathrm{k}]+n[\mathrm{k}])}^2 = \sigma_{D(e[\mathrm{k}])}^2 + \sigma_{D(n[\mathrm{k}])}^2 + 2\sigma_{D(e[\mathrm{k}])D(n[\mathrm{k}])}. \tag{16}$$

A aplicação do algoritmo de encriptação no sinal encriptado, $e[\mathrm{k}]$, resulta no sinal original $s[\mathrm{k}]$, portanto $\sigma_{D(e[\mathrm{k}])}^2 = \sigma_{m[\mathrm{k}]}^2$. Logo, a potência do sinal desencriptado é dada por

$$\sigma_z^2 = \sigma_{m[\mathrm{k}]}^2 + \sigma_{D(n[\mathrm{k}])}^2 + 2\sigma_{m[\mathrm{k}]D(n[\mathrm{k}])}. \tag{17}$$

A covariância entre $m[\mathrm{k}]$ e $D(n[\mathrm{k}])$, $\sigma_{m[\mathrm{k}]D(n[\mathrm{k}])}$ é calculada por

$$\sigma_{m[\mathrm{k}]D(n[\mathrm{k}])} = \overline{m[\mathrm{k}]D(n[\mathrm{k}])} - \overline{m[\mathrm{k}]} \cdot \overline{D(n[\mathrm{k}])}. \tag{18}$$

Como $m[\mathrm{k}]$ e $D(n[\mathrm{k}])$ são variáveis independentes, a média do produto dessas variáveis é igual ao produto das médias. Portanto, a covariância $\sigma_{m[\mathrm{k}]D(n[\mathrm{k}]))}$ é igual a 0 e a potência do sinal desencriptado é calculada por

$$\sigma_z^2 = \sigma_{m[\mathrm{k}]}^2 + \sigma_{D(n[\mathrm{k}])}^2. \tag{19}$$

A SNR é uma razão entre a potência do sinal e a potência do ruído, calculada por

$$SNR = \frac{\sigma_{m[\mathrm{k}]}^2}{\sigma_{D(n[\mathrm{k}])}^2}. \tag{20}$$

Aplicar o algoritmo de desencriptação no ruído não altera suas estatísticas pois as operações envolvidas apenas rotacionam as fases, mantendo-as com uma distribuição uniforme entre 0 e 2π, e permutam as amplitudes. Dessa maneira, a variância do ruído após o processo de desencriptação é igual à variância do ruído sem passar por nenhuma operação criptográfica, ou seja, $\sigma_{D(n[\mathrm{k}])}^2 = \sigma_{n[\mathrm{k}]}^2$. Logo, a SNR de sinais que foram criptografados e desencriptados é dada por

$$SNR = \frac{\sigma_{m[\mathrm{k}]}^2}{\sigma_{n[\mathrm{k}]}^2}. \tag{21}$$

Esse resultado mostra que o cálculo da SNR para sinais que foram encriptados pelo s-AES/s-CTR, transmitidos por um canal AWGN e desencriptados é igual ao cálculo da SNR de sinais que apenas foram transmitidos pelo mesmo canal. Dessa maneira, a técnica proposta nesse trabalho não agrega penalidades nesse cenário.

A propagação de sinais por um canal óptico foi simulada no software VPITransmissionMaker, por meio de cossimulação com o MATLAB, em colaboração com a autora de (SANTOS, 2020). Os sinais encriptados pelo software no MATLAB são enviados para o VPITransmissionMaker por cossimulação. No VPI, o sinal encriptado passa por um modulador óptico, pelo canal óptico, por um filtro óptico, por um demodulador óptico, por um filtro elétrico e é enviado novamente para o MATLAB para que o processo de desencriptação seja realizado.

O modulador óptico simula um Mach-Zender com taxa de extinção de 40dB. A simulação da propagação de sinais é realizada resolvendo-se a equação não linear de Schrödinger a partir do método de *split-step Fourier*. O canal óptico adotado nas simulações é formado por diversos enlaces de fibra óptica monomodo padrão (*standard single-mode optical fiber*, SSMF) de 80 km. A SSMF considerada tem fator de atenuação igual a 0,25 dB/km, fator de dispersão igual a 16 ps/(nm·km), inclinação da dispersão igual a 0,08 ps/(nm^2·km) e parâmetro não linear igual a 1,0 $(\mathrm{W}\cdot\mathrm{km})^{-1}$. Para compensar a atenuação e a dispersão cromática, cada enlace é composto por uma fibra SSMF de 80 km seguida de um amplificador de fibra dopada com érbio (*erbium-doped fiber amplifier*, EDFA), de uma fibra compensadora de dispersão (*dispersion-compesating fiber*, DCF) e um segundo EDFA para compensar a atenuação da DCF. A DCF considerada tem fator de atenuação igual a 0,40 dB/km, fator de dispersão igual a 16 ps/(nm·km) e parâmetro não linear igual a 1,0 $(\mathrm{W}\cdot\mathrm{km})^{-1}$. O filtro óptico é projetado para compensar o ruído adicionado na propagação do sinal. O demodulador simula um fotodetector com diodos PIN com responsividade de 1 A/W e ruído térmico de $10\cdot10^{-12}\mathrm{A}/\sqrt{\mathrm{Hz}}$ e por fim, o filtro elétrico é projetado para compensar o ruído adicionado pelo demodulador.

Foram simuladas as propagações de sinais BPSK, QPSK e 16-QAM em cenários em que os sinais foram transmitidos sem nenhum tipo de encriptação e em cenários em que os sinais foram encriptados pelo s-AES/s-CTR, propagados pelo enlace e desencriptados pelo receptor. A Fig. 27 mostra a BER em função da distância de propagação dos sinais. Comparando as curvas dos sinais que foram encriptados com as curvas dos sinais que não passaram por nenhuma operação criptográfica, é possível observar que o s-AES/s-CTR

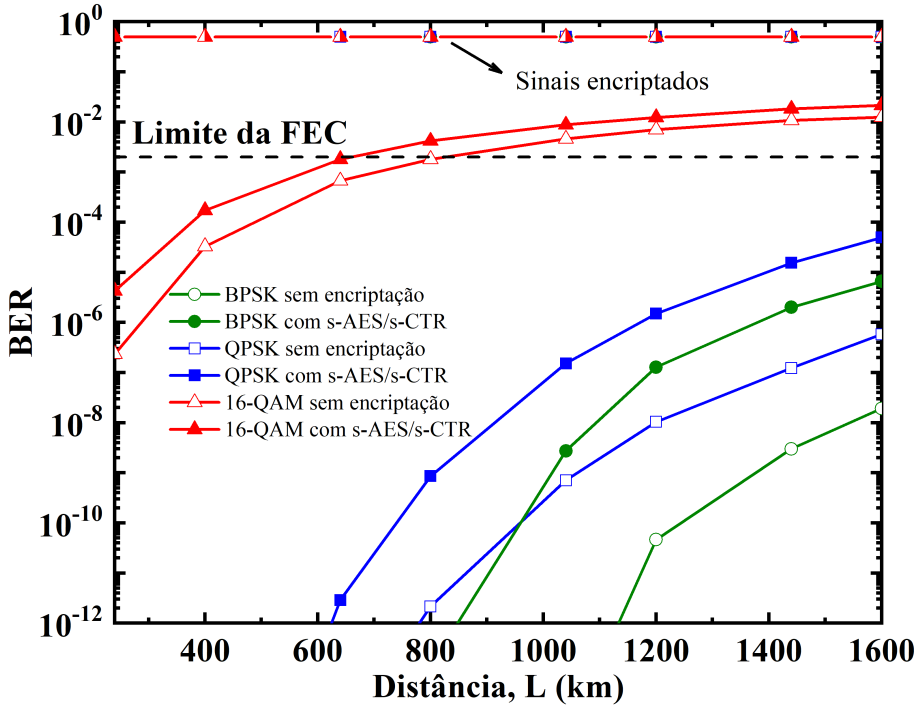


Figura 27 – BER em função da distância de propagação em um canal óptico para sinais BPSK, QPSK e 16-QAM.

agrega penalidades em todos os esquemas de modulação. A penalidade é maior para o BPSK e menor para o 16-QAM. Mesmo com a penalidade, sinais BPSK e QPSK podem ser encriptados e propagados por distâncias maiores que 1600 km sem atingir o limite da FEC.

Para sinais 16-QAM, a distância de propagação é limitada pelo limite da BER da FEC. Enquanto sinais não encriptados alcançam distâncias de até 830 km, sinais encriptados pelo s-AES/s-CTR podem ser propagados por até 650 km. Embora exista uma penalidade de aproximadamente 180 km, aplicações comerciais utilizam enlaces menores que 650 km, portanto, a técnica é compatível com redes comerciais de transmissão.

O motivo da penalidade em canais ópticos ainda está sendo avaliado. Existem algumas possibilidades que estão sendo investigadas. Por exemplo, o filtro do receptor pode estar configurado de maneira não otimizada e permitindo a passagem de um ruído adicional em sinais criptografados. Outra alternativa que está sendo avaliada é a não linearidade do funcionamento dos moduladores ópticos. A conclusão dessas investigações estão previstas para trabalhos futuros.

Os resultados apresentados nessa seção mostram que sinais criptografados pelo s-AES/s-CTR podem ser transmitidos por canais AWGN sem agregar penalidades expressivas

para os três esquemas de modulação considerados, BPSK, QPSK e 16-QAM. Já para a propagação de sinais por enlaces ópticos, verificou-se que o s-AES/s-AES agrega penalidades em todos os esquemas de modulação, porém, sinais BPSK e QPSK podem ser propagados por distâncias maiores que 1600 km e sinais 16-QAM alcançam até 650 km e portanto, o s-AES é compatível com redes comerciais. Na seção a seguir, serão discutidos os resultados referentes a segurança da técnica.

5.3 Segurança

A avaliação da segurança do s-AES/s-CTR pode ser dividida em três partes: a Subseção 5.3.1 detalha os testes para verificar se o s-AES/s-CTR atende propriedades de segurança estabelecidas em criptografia de dados, a Subseção 5.3.2 aborda a robustez da técnica contra ataques de força bruta (BFAs) e a Subseção 5.3.3 aborda a robustez da técnica contra ataques de texto escolhido (CPAs).

5.3.1 Verificação das propriedades de segurança

O s-AES/s-CTR foi projetado a partir de uma adaptação do AES e do CTR, portanto, considerou-se que as definições de segurança estabelecidas em criptografia de dados também devem ser atendidas no s-AES/s-CTR. Foram avaliadas as propriedades de difusão e confusão estabelecidas por Shannon.

A propriedade de difusão estabelece que a influência de um bit da mensagem original deve ser espalhada em vários bits da mensagem cifrada. Em acordo com essa definição, considera-se nesse trabalho que, em uma técnica que atende a propriedade de difusão, a alteração de um bit da mensagem cifrada deve alterar, aproximadamente, 50% dos bits da mensagem cifrada. Para avaliar a propriedade de difusão do s-AES/s-CTR, foi gerado um bloco de mensagem, denominado bloco de referência, e uma s-chave. O bloco de referência foi convertido para um sinal e encriptado pela s-chave. O sinal foi desencriptado, convertido em binário e armazenado. Na sequência, o primeiro bit do bloco de referência foi alterado, o novo bloco foi convertido para um sinal e encriptado pela mesma s-chave do primeiro bloco. O sinal foi desencriptado, convertido em binário e armazenado. Esse processo foi repetido até que todos os 250 bits do bloco de referência fossem alterados.

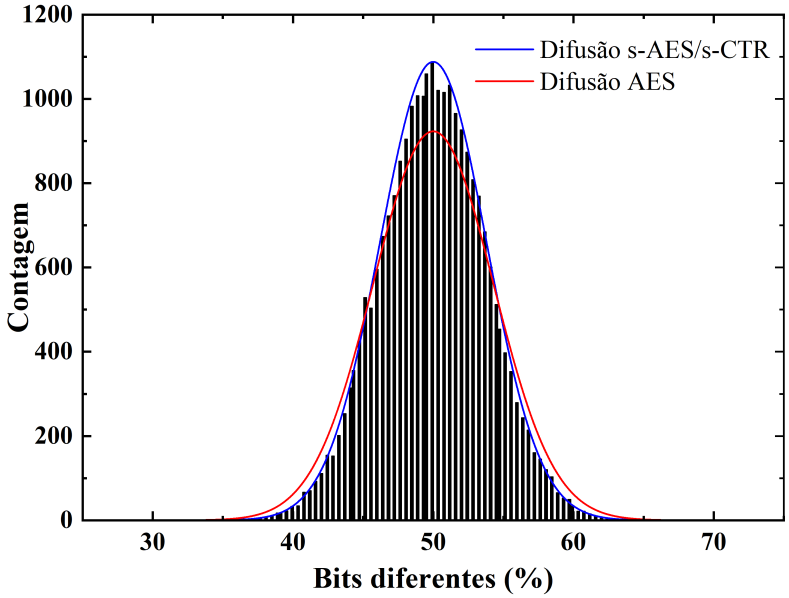


Figura 28 – Histograma de dispersão dos testes de difusão do s-AES/CTR e do AES.

Para verificar se a propriedade de difusão é atendida, cada bloco cifrado foi comparado com o bloco cifrado de referência. A porcentagem de bits diferentes entre os blocos e o bloco de referência foi armazenada para os 250 blocos. O processo foi realizado para 100 blocos de referência para alcançar precisão estatística dos resultados, totalizando 25000 valores de porcentagem de bits diferentes.

Para avaliar a diferença entre os blocos, as porcentagens encontradas foram dispostas em um histograma de dispersão. Destaca-se que, além de realizar o teste da difusão para o s-AES/s-CTR, o mesmo teste foi realizado no AES para comparar a estratégia proposta por esse trabalho com a técnica de criptografia de dados comercial. A Fig. 28 mostra o histograma de dispersão do teste de difusão do s-AES/s-CTR, bem como a gaussiana que aproxima esse histograma e a gaussiana que aproxima o histograma obtido no teste de difusão do AES. O histograma do teste de difusão do s-AES/s-CTR tem uma distribuição gaussiana centrada em 50%. Além disso, a distribuição do teste de difusão do s-AES/s-AES é mais estreita que a do AES. De fato, enquanto o desvio padrão da difusão do AES é de 0,043, o desvio padrão para o s-AES é de 0,038. Esse resultado indica que os níveis de segurança do s-AES podem ser ainda maiores que os do AES.

A propriedade de confusão estabelece que a chave criptográfica deve ser complexa de modo que a influência de um bit da chave seja espalhada em vários bits da mensagem cifrada. Nesse trabalho, considera-se que, em uma técnica que atende a propriedade de confusão, a alteração de um bit da chave ocasiona a alteração de, aproximadamente, 50%

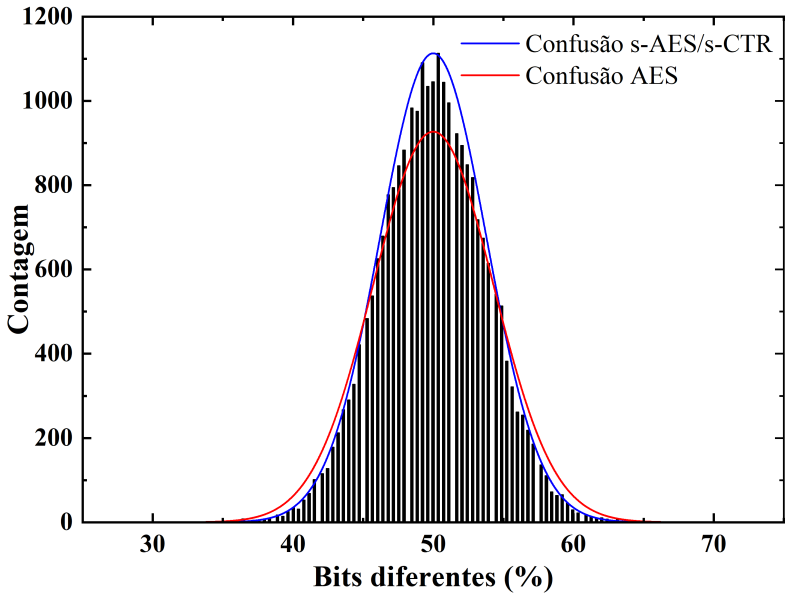


Figura 29 – Histograma de amplitude dos testes de confusão do s-AES/CTR e do AES.

dos bits da mensagem cifrada. O processo para avaliar a confusão é muito similar ao adotado nos testes da difusão, porém, o bloco de mensagem foi mantido fixo. O bloco de mensagem foi convertido em um sinal, encriptado com a s-chave, desencriptado, convertido em binário e armazenado. Foi alterado um bit da s-chave, o mesmo bloco de mensagem foi convertido em um sinal, encriptado pela nova s-chave, desencriptado, convertido em binário e armazenado. A s-chave foi alterada 250 vezes, os blocos de mensagens cifrados foram comparados com o bloco de referência cifrado para verificar a porcentagem de bits diferentes entre eles e uma nova mensagem e uma nova s-chave foram geradas. Foram realizados testes com 100 blocos de mensagens diferentes.

É importante destacar que, diferente da mensagem binária, a chave binária não tem comprimento de 250 bits. O comprimento da s-chave binária é de $8 \times 128 = 1024$ porque uma s-chave é composta por 128 fases e consideramos, nesse trabalho, que cada uma das chaves pode ser descrita por 8 bits. Dessa maneira, o teste de confusão poderia ser realizado alterando 1 bit da chave por vez por 1024 rodadas, mas optamos por realizá-lo 250 vezes e depois repetir o processo 100 vezes para que os resultados de confusão e difusão tivessem o mesmo número de dados nos histogramas apresentados.

A Fig. 29 mostra o histograma de dispersão do teste de confusão do s-AES, a gaussiana que aproxima esse histograma e a gaussiana que aproxima o histograma de dispersão do teste de confusão do AES. O resultado obtido do teste de confusão é bem similar ao da obtido para a difusão, uma gaussiana centrada em 50%. Esse resultado

mostra que o s-AES/s-CTR. além de atender a propriedade de difusão, também atende a propriedade de confusão. A gaussiana obtida para o s-AES/s-CTR também é mais estreita que para o AES, com valores de desvio padrão iguais a 0,038 e 0,043, respectivamente. Novamente, obtivemos resultados que indicam que a segurança do s-AES/s-CTR pode ser maior que a do AES.

Os resultados da verificação de propriedades de segurança estabelecidas em criptografia de dados foram bastante satisfatório pois foi provado que o s-AES/s-CTR atende às propriedades de Shannon. Dessa maneira, confirma-se que as analogias criadas para as operações do AES são capazes de prover difusão e confusão aos sinais encriptados. Na subseção a seguir será discutida a segurança da técnica contra ataques de força bruta (BFAs).

5.3.2 Robustez contra ataques de força bruta (BFAs)

O s-AES/s-CTR encripta os sinais de entrada adicionando as fases do vetor γ_i, encriptado pelo s-AES, às fases dos sinais originais e embaralhando as amostras em acordo com a ordenação das fases do vetor γ_i. Uma vez que são essas as operações criptográficas realizadas diretamente no sinal original, considera-se que um interceptador, para conseguir recuperar o sinal com qualidade razoável, deve realizar ataques no sinal encriptado para descobrir as posições e fases corretas do sinal original.

Os resultados de robustez contra BFAs levam em consideração três cenários. No primeiro cenário, assumimos que o interceptador conhece, de alguma maneira, as posições corretas das amostras e não tem nenhuma informação sobre as fases. Assim, ele terá de realizar ataques para descobrir, mesmo que com certo erro, as fases do sinal original. Em um segundo cenário, o interceptador conhece, de alguma maneira, as fases corretas do sinal original mas não conhece a posição correta das amostras. Nesse cenário, o interceptador deve realizar ataques para descobrir as posições corretas das amostras. No terceiro cenário a situação é mais realista, o interceptador não conhece informação alguma sobre as fases e posições das amostras do sinal e deve realizar ataques para descobrir ambas.

No cenário em que o interceptador conhece as posições corretas das amostras, a fase da i-ésima amostra do sinal que o interceptador tem acesso é a soma da fase da i-ésima amostra sinal original, θ_i, com a i-ésima fase do vetor γ_i, χ_i. Para recuperar o sinal

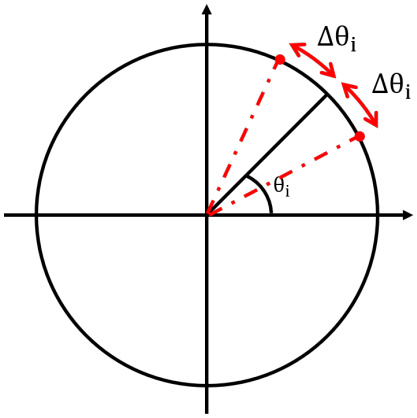


Figura 30 – Representação da fase da iésima amostra,θ_i, e o erro aceitável $\Delta\theta_i$.

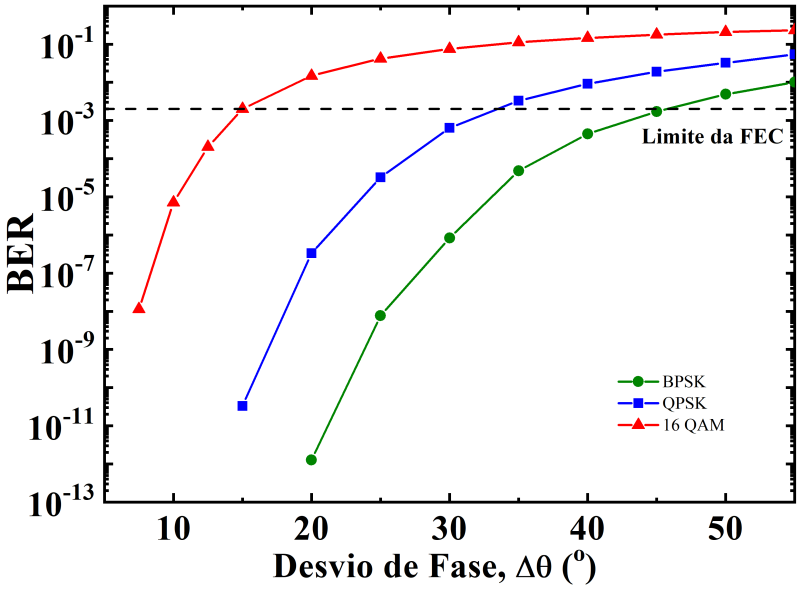


Figura 31 – BER em função do desvio de fase ($\Delta\theta$) para sinais BPSK, QPSK e 16-QAM.

sem erros, o interceptador deveria conhecer exatamente a fase χ_i e subtrair esse valor da i-ésima amostra que ele tem acesso. Porém, é possível que o interceptador erre, em alguma proporção, o valor de χ_i e consiga recuperar o sinal no limite da FEC. Considerando que o interceptador realize um ataque ao sinal criptografado em que ele atribui à i-ésima amostra o valor de fase $\theta_i \pm \Delta\theta_i$, como ilustrado na Fig. 30, é necessário descobrir qual valor de $\Delta\theta_i$ é suficiente para recuperar o sinal no limite da FEC em cada esquema de modulação.

Nas simulações computacionais, o sinal original foi mantido e adicionou-se um erro, $\Delta\theta_i$, às fases das amostras do sinal para verificar de quanto deve ser o erro máximo em cada esquema de modulação para conseguir recuperar o sinal no limite da FEC. Para alcançar precisão estatística nos testes, as simulações foram realizadas em 3000 blocos. Considerou-se que $\Delta\theta_i$ é uma variável aleatória entre $-\Delta\theta$ e $\Delta\theta$. Dessa maneira, foi adicionada a i-ésima

Tabela 2 – Número de BFAs caso o interceptador conheça as posições corretas das amostras.

	$\Delta\theta$	$N_{ataques,f}$
BPSK	45,7°	$\frac{360}{45,7}^{128} \approx 10^{114}$
QPSK	33,5°	$\frac{360}{33,7}^{128} \approx 10^{132}$
16-QAM	15°	$\frac{360}{15}^{128} \approx 10^{176}$

fatia do sinal original uma fase aleatória entre $\theta_i - \Delta\theta$ e $\theta_i + \Delta\theta$. A Fig. 31 mostra a BER em função do desvio de fase $\Delta\theta$ aplicado. Os máximos desvios de fase para o BPSK, QPSK e 16-QAM são de aproximadamente 45,7°, 33,5°e 15°, respectivamente, para o limite da FEC.

Para acertar a fase de determinada amostra com um erro de $\Delta\theta$, um interceptador deve realizar, em média, $(360/\Delta\theta)$ ataques. Para acertar a fase de todas as n_s amostras, serão necessários

$$N_{ataques,f} = \left(\frac{360}{\Delta\theta}\right)^{n_s} \tag{22}$$

ataques. Em acordo com essa equação, os números de ataques necessários para recuperar os sinais simulados no limite da FEC são apresentados na Tabela 2. Esse resultado revela que em todos os esquemas de modulação, o número de BFAs nesse cenário é maior que o do AES-256, que é da ordem $2^{256} \approx 10^{77}$. Em particular, para o 16-QAM, o número de BFAs é de aproximadamente 10^{176}, ou seja, 10^{99} vezes maior que o do AES-256.

No segundo cenário utilizado para avaliar a segurança do s-AES/s-CTR contra ataques de força bruta considerou-se que o interceptador conhece, por alguma razão, as fases corretas das amostras do sinal original mas não conhece as posições corretas. O interceptador tem acesso, então, a um sinal em que a i-ésima amostra tem amplitude e fase correta mas não está na posição correta. Dessa maneira, o ataque realizado consiste em trocar as posições de posição para tentar recuperar o sinal. Como existem n_s amostras, o número máximo de permutações que o interceptador deve realizar para acertar a posição de todas amostras é de $n_s!$. Entretanto, é possível que o interceptador acerte uma parcela das posições das amostras, N_{certas}, e consiga recuperar o sinal no limite da FEC. Nas simulações computacionais, considerou-se que as fases de todas as amostras do sinal estavam corretas e N_{certas} amostras aleatórias foram dispostas nas suas posições corretas. Assim como nas simulações do ataque anterior, foram simulados 3000 blocos. A Fig. 32 mostra a BER em

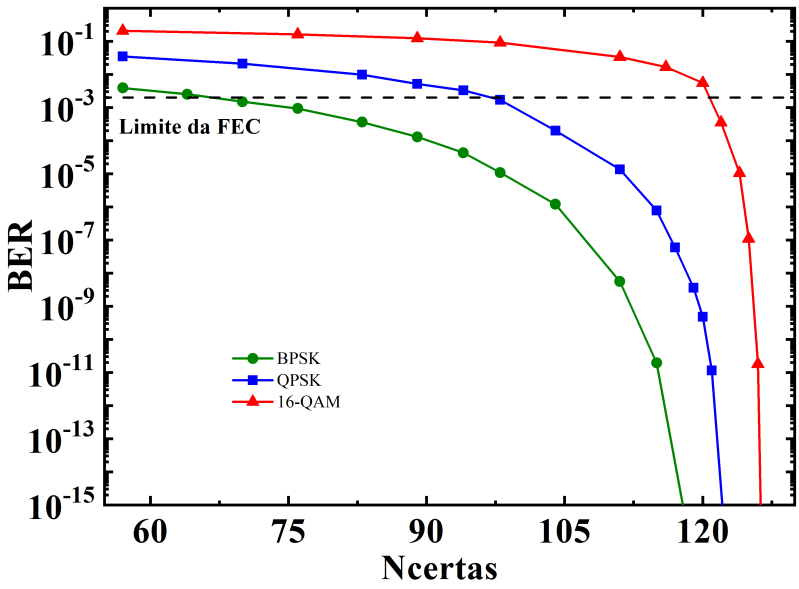


Figura 32 – BER em função do número de posições corretas para sinais BPSK, QPSK e 16-QAM.

Tabela 3 – Número de BFAs caso o interceptador conheça as fases corretas das amostras.

	N_{certas}	$N_{ataques,p}$
BPSK	66	$\frac{128!}{(128-66)!} \approx 10^{130}$
QPSK	97	$\frac{128!}{(128-97)!} \approx 10^{181}$
16-QAM	120	$\frac{128!}{(128-120)!} \approx 10^{210}$

função do número de posições corretas, N_{certas}. Para recuperar o sinal no limite da FEC, o interceptador deve acertar, pelo menos, 66 amostras em sinais BPSK, 97 amostras em sinais QPSK e 120 amostras em sinais 16-QAM.

O número de ataques necessários para recuperar o sinal no limite da FEC é menor que $n_s!$ e é calculado em acordo com

$$N_{ataques,p} = \frac{n_s!}{(n_s - N_{certas})!}. \tag{23}$$

O número de ataques necessários para recuperar o sinal no limite da FEC em cada um dos esquemas de modulações avaliados é mostrado na Tabela 3. O resultado para esse cenário mostra que, em todos os esquemas de modulação considerados, o número de BFAs necessário para recuperar o sinal no limite da FEC é maior que o do AES-256. Em particular, para recuperar sinais 16-QAM são necessários aproximadamente 10^{210}, valor que é 10^{130} vezes maior que o do AES-256.

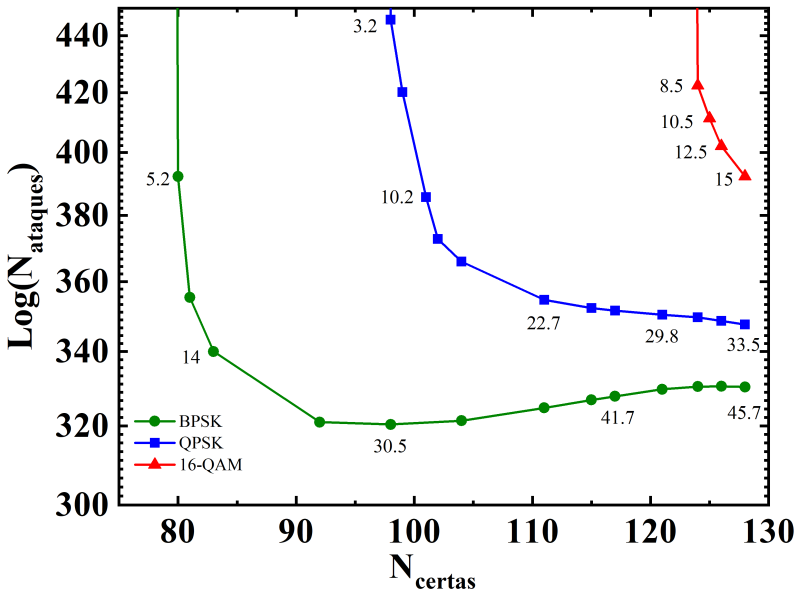


Figura 33 – Logaritmo do número de ataques em função do número de posições corretas.

No terceiro e mais realista dos cenários, o interceptador não conhece nem as fases corretas nem as posições corretas das amostras do sinal. Dessa maneira, existe um compromisso entre a quantidade de posições corretas das amostras e o desvio de fase aplicado para que o sinal possa ser recuperado no limite da FEC. A fórmula para o cálculo do número BFAS nesse cenário em que o interceptador deve realizar ataques tanto nas fases quanto nas posições das amostras é dada por

$$N_{ataques} = N_{ataques,f} \cdot N_{ataques,p} = \left(\frac{360}{\Delta\theta}\right)^{n_s} \frac{n_s!}{(n_s - N_{certas})!}. \tag{24}$$

As simulações computacionais adotaram os dois métodos dos cenários anteriores em conjunto. Ou seja, foi aplicado um desvio de fase $\Delta\theta$ às fases corretas do sinais e N_{certas} amostras foram desembaralhadas corretamente. Nesse teste, os valores de $\Delta\theta$ e N_{certas} foram variados até alcançar limite da FEC fosse atingido. Como existe um compromisso entre $\Delta\theta$ e N_{certas}, diversos pares de valores podem atingir o limite da FEC. O logaritmo do número de ataques foi calculado para esses pontos e é apresentado na Fig. 33 em função de N_{certas}. Os valores de $\Delta\theta$ correspondentes aos pontos estão apresentados próximos a eles. Esse resultado indica que existe um limite mínimo de N_{certas} que o interceptador precisa descobrir para conseguir recuperar o sinal. O número mínimo de amostras na posição correta para recuperar o sinal é de 80 amostras para sinais BPSK, de 98 amostras para sinais QPSK e de 124 amostras para sinais 16-QAM.

Tabela 4 – Número mínimo de BFAs para recuperar sinais BPSK, QPSK e 16-QAM.

	$\Delta\theta$	N_{certas}	$N_{ataques}$
BPSK	30,5°	98	$\left(\frac{360}{30,5^\circ}\right)^{128} \frac{128!}{(128-98)!} \approx 10^{320}$
QPSK	33,5°	128	$\left(\frac{360}{33,5^\circ}\right)^{128} \frac{128!}{(128-128)!} \approx 10^{347}$
16-QAM	15°	128	$\left(\frac{360}{15^\circ}\right)^{128} \frac{128!}{(128-128)!} \approx 10^{392}$

Ainda analisando a Fig. 33, para cada esquema de modulação existe um valor mínimo do número de BFAs para o interceptador garantir a recuperação do sinal no limite da FEC. A Tabela 4 mostra os valores de $\Delta\theta$, N_{certas} e o número mínimo de ataques para sinais BPSK, QPSK e 16-QAM. Verifica-se que, para todos os esquemas de modulação, o número mínimo de BFAs é bem maior que o número de BFAs do AES-256. Particularmente, para o esquema de modulação que apresenta o menor número de BFAs, o BPSK, o número mínimo de BFAs é aproximadamente 10^{320}. Portanto, a segurança contra ataques de força bruta em sinais encriptados pelo s-AES/s-CTR é, no mínimo, 10^{243} vezes maior que a do AES.

Os resultados dessa subseção mostraram que, além do s-AES/s-CTR ser seguro contra BFAs, apresenta números de ataques bastante superiores aos do padrão AES-256. Nos cenários em que o interceptador conhece informações sobre o sinal, a segurança do s-AES é da ordem de 10^{100} vezes maior que a do AES. Porém em um cenário mais realista, em que o interceptador não conhece nenhuma informação sobre o sinal, a técnica proposta apresenta robustez à ataques de força bruta, no mínimo, 10^{243} maior que a do AES. Na próxima seção será discutida a robustez do s-AES/s-CTR contra CPAs.

5.3.3 Robustez contra ataques de texto escolhido (CPAs)

Em um ataque de texto escolhido, o interceptador assume um jogo contra o algoritmo de encriptação em que são enviadas duas mensagens ao algoritmo de encriptação, essas são encriptadas e enviadas para o interceptador. Em algoritmo robusto contra CPAs, o interceptador não consegue distinguir qual das mensagens cifradas corresponde a qual das mensagens originais. A robustez contra CPAs deve ser provada matematicamente. A prova matemática da robustez contra CPAs não faz parte do escopo desse trabalho devido ao tempo, mas compõe os tópicos que serão abordados nas próximas etapadas desse trabalho.

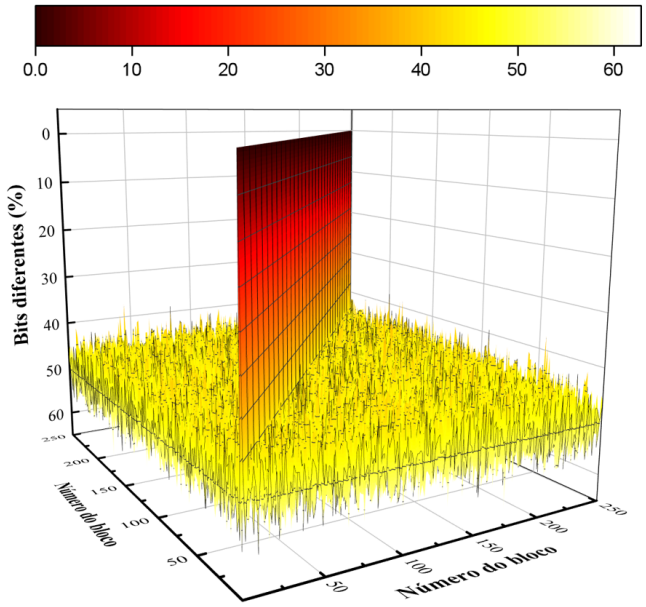


Figura 34 – *Colormap* para robustez contra CPA (16-QAM).

Nesse trabalho, verificamos se a encriptação de sinais iguais resulta em sinais encriptados diferentes.

Nas simulações computacionais, foi gerado um bloco de mensagem, que foi convertido para sinal, encriptado por uma s-chave, desencriptado e convertido para binário. Esse processo foi repetido 251 vezes para o mesmo bloco e a mesma s-chave e os blocos encriptados foram comparados entre eles. O resultado é uma matriz 250x250 com as porcentagens de bits diferentes entre os blocos. Essa matriz é apresentada em um *colormap* na Fig. 34. A diagonal da matriz é igual a 0 pois nesses casos compara-se cada bloco com ele mesmo. Todos os outros valores estão próximos de 50%, ou seja, temos um indicativo de que o s-AES/s-CTR pode ser probabilístico e robusto contra CPAs.

Os resultados discutidos no decorrer desse capítulo foram bastante satisfatórios. Mostrou se que o s-AES/s-CTR encripta e desencripta os sinais corretamente, então interceptadores não conseguem ter acesso aos sinais originais com facilidade. A propagação de sinais encriptados pelo s-AES/s-CTR mostrou que, em canais AWGN, nenhuma penalidade é agregada aos sinais e que, em canais ópticos, mesmo com certa penalidade, o s-AES/s-CTR é compatível com redes de até 650 km. Com respeito a segurança da técnica, o s-AES/s-CTR provê as propriedades de difusão e confusão aos sinais encriptados. A técnica proposta tem boa segurança contra BFAs e inclusive, apresenta resultados de segurança contra BFAs maiores que o do AES-256. Por fim, os resultados indicam que o

s-AES/s-CTR pode ser probabilístico e robusto contra CPAs. No próximo capítulo são apresentadas as considerações finais desse trabalho.

6 Conclusões

A proposta principal desse trabalho foi desenvolver uma nova técnica de criptografia espectral de sinais análoga a um padrão de criptografia de dados, o AES. A nova técnica, denominada s-AES, apresentou bons resultados e tem bastante potencial para aplicação. Além da adaptação e desenvolvimento do s-AES, o modo de operação CTR, definido e utilizado em criptografia de dados, também foi adaptado para uma versão que atua sob sinais, chamada de s-CTR, a fim de aleatorizar os sinais encriptados para que a estratégia final desse projeto fosse robusta contra CPAs e possibilitasse a reutilização de chaves criptográficas. A adaptação do AES para o s-AES foi desenvolvida a partir das analogias estabelecidas no Capítulo 4. Essas analogias não consideram que as tabelas de substituição do AES foram construídas de maneira que minimizassem a eficiência de ataques diferenciais. De fato, no melhor de nosso conhecimento, ataques diferenciais ainda não foram estudados no contexto de criptografia de sinais.

Os resultados obtidos mostram que sinais encriptados pelo s-AES/s-CTR não podem ser recuperados com BER menor que 0,5 sem a realização de algum tipo de ataque. Um interceptador, com acesso ao sinal encriptado, se depara com um sinal com um espectro de amplitudes aproximadamente branco, em que as amplitudes do sinal original estão embaralhadas e com um espectro de fases em que as fases do sinal original estão rotacionadas e embaralhadas. A constelação de um sinal encriptado é uma mancha circular em que os símbolos originais não são identificados, cujas distribuições de amplitude no eixo I e no eixo Q correspondem à gaussianas.

Com relação a transmissão de sinais criptografados, o s-AES/s-CTR também apresentou bons resultados. Sinais BPSK, QPSK e 16-QAM podem ser transmitidos por canais AWGN sem agregar nenhum tipo de penalidade. Em enlaces ópticos, existem penalidades para todos os esquemas de modulação, porém, sinais BPSK e QPSK podem ser propagados em distâncias maiores que 1200 km sem atingir o limite da FEC. Sinais 16-QAM, mesmo com 180 km de penalidade, podem ser propagados por canais ópticos de até 650 km. Dessa maneira, o s-AES/s-CTR é compatível com redes comerciais de transmissão. As razões que levaram a penalidades em canais ópticas ainda estão sendo avaliadas e podem estar relacionadas às configurações do receptor.

A segurança do s-AES/s-CTR também foi avaliada nesse trabalho. Foi verificado que o s-AES/s-CTR provê difusão aos sinais cifrados. Os resultados mostram que a alteração de um bit da mensagem ocasiona a alteração de, aproximadamente, 50% dos bits da mensagem cifrada. A propriedade de confusão também é atingida, ou seja, a alteração de um bit da s-chave leva a alteração de, aproximadamente, 50% dos bits da mensagem cifrada. O desvio padrão do histograma de dispersão da difusão e confusão do s-AES/s-CTR, com distribuição gaussiana, é de 0,038, enquanto o desvio padrão para o AES é de 0,043. Esse resultado mostra que o s-AES/s-CTR pode ser mais seguro que o AES com relação a essas propriedades.

O s-AES/s-CTR tem boa robustez contra ataques de força bruta (BFA). Os resultados obtidos mostram que, em cenários em que o interceptador conhece, por alguma razão, as posições corretas de todas as amostras do sinal, o número de BFAs necessário para conseguir recuperar um sinal 16-QAM no limite da FEC é de 10^{176}. Em cenários em que o interceptador conhece as posições das amostras mas não tem informações sobre as fases das amostras, o número de BFAs para recuperar sinais 16-QAM é de 10^{210}. Por fim, em um cenário realista em que o interceptador não tem informações sobre as fases e sobre as posições corretas das amostras, são necessários, no mínimo, 10^{392} ataques de força bruta. Comparando com o AES, que apresenta número de FBAs igual a 10^{77}, o s-AES/s-CTR apresenta segurança contra BFAs maior mesmo em cenários conservadores. Em um cenário mais realista, a robustez contra BFAs do s-AES/s-CTR é aproximadamente 10^{243} vezes maior que a do AES.

Com relação a CPAs, verificou-se que o modo de operação s-CTR aleatoriza as mensagens cifradas e a encriptação de dois sinais com a mesma s-chave leva a sinais encriptados sem relação entre si, ou seja, a técnica pode ser probabilística e robusta contra CPAs. A robustez contra CPAs deve ser comprovada matematicamente. Além disso, deve ser verificada a robustez da técnica contra ataques mais elaborados. Dentre os possíveis ataques, destaca-se aqui a necessidade de realizar testes de criptoanálise linear e diferencial, bem como verificar a robustez da estratégia contra ataques algébricos. O estudo aprofundado da segurança do s-AES/s-CTR será realizado em trabalhos futuros.

Além de verificar profundamente a segurança do s-AES/s-CTR, deve-se investigar se as penalidades encontradas na simulação da transmissão de sinais criptografados por canais ópticos são causadas pelo s-AES/s-CTR ou pelas configurações do receptor. Por fim, o s-AES/s-CTR deve ser implementado experimentalmente e em campo. Para testes em

campo, a técnica pode ser implementada em *hardware* em um FPGA *(field programmable gate array)*, por exemplo.

Os resultados de simulação obtidos sugerem que o s-AES/s-CTR seja uma técnica eficiente, robusta e com grande potencial para aplicações comerciais. No melhor de nosso conhecimento, essa é a primeira técnica de criptografia de sinais que possibilita a reutilização de chaves e provê, comprovadamente, as propriedades de difusão e confusão aos sinais criptografados. De fato, a técnica proposta nesse trabalho compõe uma comunicação de invenção que está sendo redigida para ser encaminhada à Agência Unesp de Inovação (AUIN) para solicitação do depósito de patente.

6.1 Lista de publicações

A. Trabalhos Publicados

1. Santos, M. de O.; Souza, W. S.; Bragagnolle, T. de A.; Bobadilla, L. D. B.; Aldaya, I.; Prado, A. J. do; Ferreira, A. A.; Bonani, L. H.; Abbade, M. L. F. All-optical Spectral Shuffling Applied to 16-QAM Signals. 2019 SBFoton International Optics and Photonics Conference (SBFoton IOPC), 2019.
2. Souza, W. S.; Nogueira, M. P.; Rodrigues, I. E. L.; Santos, M. de O.; Bonani, L. H.;Aldaya, I.; Abbade, M. L. F. Spectral Shuffling with Phase Encoding and Dynamic Keys Applied to Transparent Optical Network Signals. 22nd International Conference on Transparent Optical Networks - ICTON 2020.
3. Abbade, M. L. F.; Souza, W. S.; Nogueira, M. P.; Rodrigues, I. E. L.; Santos, M. de O.; Bonani, L. H.; Aldaya, I. Signal Encryption Opportunities for Photonic Networks. Advanced Photonics Congress 2020 - APC 2020.

B. Trabalhos em Preparação

1. Abbade, M. L. F.; Souza, W. S.; Santos, M. O.; Prado A. J.; Aldaya, I. Encryption of Baseband Signals with Sample Spectral Encoding and Binary Dynamic Keys. A ser submetido ao IEEE Access.

Referências[1]

ABBADE, M.; JR, L. F.; MESSANI, C.; TANIGUTI, G.; FAGOTTO, E.; FONSECA, I. All-optical cryptography through spectral amplitude and delay encoding. *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, SciELO Brasil, v. 12, n. 2, p. 376–397, 2013. Citado na página 54.

ABBADE, M. L.; ASSIS, G. H.; ALVES, C. J.; MESSANI, C. A.; FAGOTTO, E. A.; CVIJETIC, M. All-optical phase and delay spectral encoding of signals with advanced modulation formats. In: IEEE. *2014 16th International Conference on Transparent Optical Networks (ICTON)*. [S.l.], 2014. p. 1–4. Citado 3 vezes nas páginas 23, 24 e 51.

ABBADE, M. L.; CVIJETIC, M.; MESSANI, C. A.; ALVES, C. J.; TENENBAUM, S. All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys. *Applied optics*, Optical Society of America, v. 54, n. 14, p. 4359–4365, 2015. Citado 3 vezes nas páginas 23, 24 e 51.

ABBADE, M. L.; NOGUEIRA, M. P.; SANTOS, M. O.; FAGOTTO, E. A.; BONANI, L. H.; ALDAYA, I. Dsp-based multi-channel spectral shuffling applied to optical networks. *IEEE Photonics Technology Letters*, IEEE, v. 32, n. 3, p. 154–157, 2019. Citado 4 vezes nas páginas 23, 24, 51 e 56.

ABBADE, M. L. F.; BOBADILLA, L. D. B.; CARVALHO, D. O. de; FERREIRA, A. A.; BONANI, L. H.; ALDAYA, I. All-optical encryption using multi-channel spectral shuffling. *IEEE Photonics Technology Letters*, IEEE, v. 31, n. 1, p. 98–101, 2018. Citado 3 vezes nas páginas 23, 24 e 51.

ABBADE, M. L. F.; BOBADILLA, L. D. B.; MARTÃO, V. B.; CARVALHO, D. O. D.; FERREIRA, A. A.; BONANI, L. H. Double-lock strategy applied to optical spectral phase and delay encoding. In: IEEE. *2017 SBMO/IEEE MTT-S International Microwave And Optoelectronics Conference (IMOC)*. [S.l.], 2017. p. 1–5. Citado 3 vezes nas páginas 23, 24 e 51.

ABBADE, M. L. F.; LESSA, L. S.; SANTOS, M. de O.; PRADO, A. J. do; ALDAYA, I. A new DSP-based physical layer encryption technique applied to passive optical networks. In: IEEE. *2018 20th International Conference on Transparent Optical Networks (ICTON)*. [S.l.], 2018. p. 1–4. Citado 3 vezes nas páginas 23, 24 e 51.

BARKAN, E.; BIHAM, E.; KELLER, N. Instant ciphertext-only cryptanalysis of gsm encrypted communication. In: SPRINGER. *Annual international cryptology conference*. [S.l.], 2003. p. 600–616. Citado na página 28.

BENNETT, C. H.; BESSETTE, F.; BRASSARD, G.; SALVAIL, L.; SMOLIN, J. Experimental quantum cryptography. *Journal of cryptology*, Springer, v. 5, n. 1, p. 3–28, 1992. Citado 2 vezes nas páginas 23 e 45.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. *IEEE Internetional Conference on Computers, Systems and Signal Processing*, v. 175, p. 8, 1984. Citado 2 vezes nas páginas 23 e 45.

[1] De acordo com a Associação Brasileira de Normas Técnicas. NBR 6023.

BENNETT, C. H.; BRASSARD, G.; EKERT, A. K. Quantum cryptography. *Scientific American*, JSTOR, v. 267, n. 4, p. 50–57, 1992. Citado 2 vezes nas páginas 23 e 45.

BOGDANOV, A.; KHOVRATOVICH, D.; RECHBERGER, C. Biclique cryptanalysis of the full AES. In: SPRINGER. *International Conference on the Theory and Application of Cryptology and Information Security*. [S.l.], 2011. p. 344–371. Citado na página 38.

CORNEJO, J. A.; PEREZ, C. E. *et al.* WDM-compatible channel scrambling for secure high-data-rate optical transmissions. *Journal of lightwave technology*, IEEE, v. 25, n. 8, p. 2081–2089, 2007. Citado 3 vezes nas páginas 23, 24 e 51.

DAEMEN, J.; RIJMEN, V. *The design of Rijndael: AES-the Advanced Encryption Standard*. [S.l.]: Springer Science & Business Media, 2013. Citado 2 vezes nas páginas 37 e 38.

EKERT, A. K. Quantum cryptography based on Bell's theorem. *Physical review letters*, APS, v. 67, n. 6, p. 661, 1991. Citado 3 vezes nas páginas 23, 45 e 47.

FIPS, N. 197: Announcing the Advanced Encryption Standard. *...Technology Laboratory, National Institute of Standards...*, National Institute of Standards and Technology (NIST), p. 1–47, 2001. Citado 3 vezes nas páginas 22, 33 e 34.

FOK, M. P.; WANG, Z.; DENG, Y.; PRUCNAL, P. R. Optical layer security in fiber-optic networks. *IEEE Transactions on Information Forensics and Security*, IEEE, v. 6, n. 3, p. 725–736, 2011. Citado na página 23.

FOROUZAN, B. A. *Cryptography & network security*. [S.l.]: McGraw-Hill, Inc., 2007. Citado 2 vezes nas páginas 31 e 32.

GENG, C.; YANG, X.; SUN, W.; HU, W. Multi-fold physical layer data encryption using chaotic frequency hopping. In: IEEE. *2018 20th International Conference on Transparent Optical Networks (ICTON)*. [S.l.], 2018. p. 1–4. Citado 3 vezes nas páginas 23, 24 e 47.

GILMORE, J. *EFF builds DES cracker that proves that data encryption standard is insecure*. [S.l.]: EFF press release, 1998. Citado na página 33.

GOLDWASSER, S.; MICALI, S. Probabilistic encryption. *Journal of computer and system sciences*, Elsevier, v. 28, n. 2, p. 270–299, 1984. Citado na página 29.

HOU, T.; YI, L.; YANG, X.; KE, J.; HU, Y.; YANG, Q.; ZHOU, P.; HU, W. Maximizing the security of chaotic optical communications. *Optics express*, Optical Society of America, v. 24, n. 20, p. 23439–23449, 2016. Citado 3 vezes nas páginas 23, 24 e 47.

HU, X.; YANG, X.; SHEN, Z.; HE, H.; HU, W.; BAI, C. Chaos-based partial transmit sequence technique for physical layer security in ofdm-pon. *IEEE Photonics Technology Letters*, IEEE, v. 27, n. 23, p. 2429–2432, 2015. Citado 3 vezes nas páginas 23, 24 e 47.

KATZ, J.; LINDELL, Y. *Introduction to modern cryptography*. [S.l.]: CRC press, 2014. Citado 7 vezes nas páginas 22, 27, 28, 29, 39, 40 e 41.

KE, J.; YI, L.; HOU, T.; HU, W. Key technologies in chaotic optical communications. *Frontiers of Optoelectronics*, Springer, v. 9, n. 3, p. 508–517, 2016. Citado 3 vezes nas páginas 23, 24 e 47.

KELLY, T. The myth of the skytale. *Cryptologia*, Taylor & Francis, v. 22, n. 3, p. 244–260, 1998. Citado na página 20.

Lathi, B. P.; Ding, Z. *Sistemas de Comunicações Analógicos e Digitais Modernos*. [S.l.]: LTC, 2012. (4). Bibliografia: p. 131–132. ISBN 8521620276. Citado na página 71.

LIAO, S.-K.; CAI, W.-Q.; LIU, W.-Y.; ZHANG, L.; LI, Y.; REN, J.-G.; YIN, J.; SHEN, Q.; CAO, Y.; LI, Z.-P. *et al.* Satellite-to-ground quantum key distribution. *Nature*, Nature Publishing Group, v. 549, n. 7670, p. 43, 2017. Citado 3 vezes nas páginas 23, 24 e 47.

LIDL, R.; NIEDERREITER, H. *Introduction to finite fields and their applications*. [S.l.]: Cambridge university press, 1994. Citado na página 34.

LU, Y.; MEIER, W.; VAUDENAY, S. The conditional correlation attack: A practical attack on bluetooth encryption. In: SPRINGER. *Annual International Cryptology Conference*. [S.l.], 2005. p. 97–117. Citado na página 28.

LUCAMARINI, M.; YUAN, Z. L.; DYNES, J. F.; SHIELDS, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, Nature Publishing Group, v. 557, n. 7705, p. 400–403, 2018. Citado na página 46.

MAO, Y.; WANG, B.-X.; ZHAO, C.; WANG, G.; WANG, R.; WANG, H.; ZHOU, F.; NIE, J.; CHEN, Q.; ZHAO, Y. *et al.* Integrating quantum key distribution with classical communications in backbone fiber network. *Optics express*, Optical Society of America, v. 26, n. 5, p. 6010–6020, 2018. Citado 3 vezes nas páginas 23, 24 e 47.

MENEZES, A. J.; KATZ, J.; OORSCHOT, P. C. V.; VANSTONE, S. A. *Handbook of applied cryptography*. [S.l.]: CRC press, 1996. Citado 3 vezes nas páginas 21, 28 e 30.

NGO, H. H.; WU, X.; LE, P. D.; WILSON, C.; SRINIVASAN, B. Dynamic key cryptography and applications. *IJ Network Security*, v. 10, n. 3, p. 161–174, 2010. Citado 2 vezes nas páginas 55 e 57.

ODEN, J.; LAVROV, R.; CHEMBO, Y. K.; LARGER, L. Multi-Gbit/s optical phase chaos communications using a time-delayed optoelectronic oscillator with a three-wave interferometer nonlinearity. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, AIP Publishing, v. 27, n. 11, p. 114311, 2017. Citado 3 vezes nas páginas 23, 24 e 47.

PFLEEGER, C. P. *Security in computing*. [S.l.]: Pearson Education India, 2009. Citado na página 28.

PUB, N. F. 46-3. Data Encryption Standard. *Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce*, 1977. Citado 2 vezes nas páginas 22 e 31.

RIJMEN, V.; DAEMEN, J. Advanced Encryption Standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, p. 19–22, 2001. Citado 2 vezes nas páginas 22 e 33.

SANTOS, M. de O. *Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas*. Dissertação (Mestrado em Engenharia Elétrica) — Universidade Estadual Paulista (UNESP), São João da Boa Vista, 2020. Citado 6 vezes nas páginas 23, 24, 51, 53, 55 e 75.

SANTOS, M. de O.; SOUZA, W. S.; BRAGAGNOLLE, T. de A.; ALDAYA, L. D. B. B. I.; PRADO, A. J. do; FERREIRA, A. A.; ABBADE, M. L. F.; NASCIMENTO, L. H. B. do. All-optical spectral shuffling applied to 16-qam signals. In: IEEE. *2019 SBFoton International Optics and Photonics Conference (SBFoton IOPC)*. [S.l.], 2019. p. 1–5. Citado 3 vezes nas páginas 23, 24 e 51.

SCARFONE, K.; JANSEN, W.; TRACY, M. Guide to general server security. *NIST Special Publication*, v. 800, n. s 123, 2008. Citado na página 20.

SCHNEIER, B. *Applied Cryptography*. [S.l.]: John Wiley & Sons., 1996. Citado na página 31.

SHAFI, G.; SILVIO, M. Probabilistic encryption & how to play mental poker keeping secret all partial information. In: *14th ACM STOC*. [S.l.: s.n.], 1982. v. 365. Citado na página 22.

SHANNON, C. E. Communication theory of secrecy systems. *Bell system technical journal*, Wiley Online Library, v. 28, n. 4, p. 656–715, 1949. Citado 2 vezes nas páginas 21 e 22.

SINGH, A.; AGARWAL, P.; CHAND, M. Analysis of development of dynamic S-box generation. 2017. Citado na página 36.

SMART, N. P. The enigma machine. In: *Cryptography Made Simple*. [S.l.]: Springer, 2016. p. 133–161. Citado na página 21.

SOUZA, W. S.; NOGUEIRA, M. P.; RODRIGUES, I. E. L.; SANTOS, M. O.; BONANI, L. H.; ALDAYA, I.; ABBADE, M. L. F. Spectral shuffling with phase encoding and dynamic keys applied to transparente optical network signals. In: IEEE. *2020 22nd International Conference on Transparent Optical Networks (ICTON)*. [S.l.], 2020. Citado 4 vezes nas páginas 23, 24, 51 e 57.

STINSON, D. R.; PATERSON, M. *Cryptography: theory and practice*. [S.l.]: CRC press, 2018. Citado na página 31.

SULTAN, A.; YANG, X.; HAJOMER, A. A.; HU, W. Chaotic constellation mapping for physical-layer data encryption in OFDM-PON. *IEEE Photonics Technology Letters*, IEEE, v. 30, n. 4, p. 339–342, 2018. Citado 7 vezes nas páginas 9, 23, 24, 47, 48, 49 e 50.

TANENBAUM, A. s; WETHERALL, D. J. Computer networks. Pearson, 2010. Citado na página 21.

TychopouloS, A.; Koufopaulou, O.; Tomkos, I. FEC in optical communications - A tutorial overview on the evolution of architectures and the future prospects of outband and inband FEC for optical communications. *Circuits and Devices Magazine, IEEE*, v. 22, p. 79 – 86, 12 2006. Citado na página 73.

WAGNER, N. R. The laws of cryptography with java code. *Available online at Neal Wagner's home page*, 2003. Citado na página 35.

WANG, C.; SKLAR, D.; JOHNSON, D. Forward error-correction coding. *Crosslink*, v. 3, n. 1, p. 26–29, 2001. Citado na página 53.

WANG, Z.; PRUCNAL, P. R. Optical steganography over a public DPSK channel. In: IEEE. *2010 23rd Annual Meeting of the IEEE Photonics Society*. [S.l.], 2010. p. 88–89. Citado na página 44.

WOOTTERS, W. K.; ZUREK, W. H. A single quantum cannot be cloned. *Nature*, Springer, v. 299, n. 5886, p. 802–803, 1982. Citado na página 45.

WU, B.; WANG, Z.; TIAN, Y.; FOK, M. P.; SHASTRI, B. J.; KANOFF, D. R.; PRUCNAL, P. R. Optical steganography based on amplified spontaneous emission noise. *Optics express*, Optical Society of America, v. 21, n. 2, p. 2065–2071, 2013. Citado na página 44.

WU, H.; PRENEEL, B. Key recovery attack on py and pypy with chosen ivs. *eSTREAM, ECRYPT Stream Cipher Project, Report*, Citeseer, v. 52, p. 2006, 2006. Citado na página 28.

WU, H.; PRENEEL, B. Differential-linear attacks against the stream cipher phelix. In: SPRINGER. *International Workshop on Fast Software Encryption*. [S.l.], 2007. p. 87–100. Citado na página 28.

YANG, X.; SHEN, Z.; HU, X.; HU, W. Chaotic encryption algorithm against chosen-plaintext attacks in optical ofdm transmission. *IEEE Photonics Technology Letters*, IEEE, v. 28, n. 22, p. 2499–2502, 2016. Citado 6 vezes nas páginas 9, 23, 24, 47, 48 e 49.

YI, L.; KE, J.; XIA, G.; HU, W. Phase chaos generation and security enhancement by introducing fine-controllable dispersion. *Journal of Optics*, IOP Publishing, v. 20, n. 2, p. 024004, 2018. Citado 3 vezes nas páginas 23, 24 e 47.

YIN, H.-L.; CHEN, T.-Y.; YU, Z.-W.; LIU, H.; YOU, L.-X.; ZHOU, Y.-H.; CHEN, S.-J.; MAO, Y.; HUANG, M.-Q.; ZHANG, W.-J. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters*, APS, v. 117, n. 19, p. 190501, 2016. Citado 3 vezes nas páginas 23, 24 e 47.

ZHANG, Q.; TAKESUE, H.; HONJO, T.; WEN, K.; HIROHATA, T.; SUYAMA, M.; TAKIGUCHI, Y.; KAMADA, H.; TOKURA, Y.; TADANAGA, O. *et al.* Megabits secure key rate quantum key distribution. *New Journal of Physics*, IOP Publishing, v. 11, n. 4, p. 045010, 2009. Citado na página 46.