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

MELISSA DE OLIVEIRA SANTOS

Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas

São João da Boa Vista
2020

MELISSA DE OLIVEIRA SANTOS

Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas

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

São João da Boa Vista

2020

S237c

Santos, Melissa de Oliveira

Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas / Melissa de Oliveira Santos. -- São João da Boa Vista, 2020

65 p. : 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. Comunicações ópticas. 2. Segurança de sistemas. 3. Fibras 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

Câmpus de Sorocaba

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas

AUTORA: MELISSA DE OLIVEIRA SANTOS
ORIENTADOR: MARCELO LUÍS FRANCISCO ABBADE

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

Prof. Dr. MARCELO LUÍS FRANCISCO ABBADE
Coordenadoria de Curso de Engenharia Eletronica e de Telecomunicações / Câmpus de São João da Boa Vista

Prof. Dr. IVAN ARITZ ALDAYA GARDE
Coordenadoria de Curso de Engenharia Eletrônica e de Telecomunicações / Câmpus de São João da Boa Vista

Prof. Dr. MURILO ARAUJO ROMERO
Engenharia Elétrica e Computação / EESC/USP

Sorocaba, 29 de maio de 2020

Dedico esse trabalho à Deus, que age em mim de forma acolhedora, manifestando todo o meu potencial. Também dedico a todas as pessoas que, de alguma forma, me fizeram sentir mais próxima da Sua presença.

Agradecimentos

Em primeiro lugar agradeço à Deus, energia poderosa e transformadora dentro de mim, e à todas aquelas pessoas que me levaram para mais perto dEle.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior -– Brasil (CAPES) – Código de Financiamento 001 entre 01/07/19 e 30/09/19. Entre 01/11/2018 e 31/05/2020, esse trabalho foi financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), no escopo do processo 2018/12756-6. Agradeço à ambas agências pelo financiamento que viabilizou a realização desse trabalho.

À toda minha família, por comemorar comigo em cada uma das minhas conquistas. Em especial aos meus sobrinhos, Bernardo, Benjamin, Caio e Sara, e ao meu cachorro, Shoyu, que juntos são meu coração fora do corpo.

Aos meus verdadeiros amigos e colegas de pesquisa, pelos medos e êxitos compartilhados. Sinto a presença de vocês mesmo quando distantes.

Aos professores Marcelo Luís Francisco Abbade, Ivan Aritz Aldaya Garde e Afonso José do Prado, pelo apoio, incentivo e orientação, para deixar o meu trabalho o melhor possível.

Por fim, a todos que direta ou indiretamente fizeram parte dessa etapa, deixo aqui o meu muito obrigada.

"Quando a mudança começa em ti, já começaste a mudar o mundo..."

(Osho)

Resumo

SANTOS, Melissa de Oliveira. **Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas**. 2020. 65 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, 2019.

O objetivo desse projeto é propor e avaliar a aplicação de uma nova técnica de criptografia de sinais para sistemas de comunicações ópticas. A técnica consiste em utilizar processamento digital de sinais para: i) dividir um sinal de entrada em várias fatias espectrais, ii) aplicar um desvio de fase a cada fatia, iii) embaralhar essas fatias entre si e iv) multiplexar espectralmente todas as fatias, v) para gerar um sinal banda-base de saída que é uma versão encriptada (distorcida) do sinal de entrada. Essa técnica foi denominada como criptografia de codificação espectral de fase e embaralhamento intracanal por processamento digital de sinais (*spectral phase encoding and scrambling cryptography by digital signal processing*, DSP-SPE-Scr). O sinal em banda-base criptografado é então modulado em uma portadora óptica e propagado por uma rede óptica transparente. Resultados obtidos sugerem que a técnica é muito segura contra ataques de força bruta. Além disso, apesar do sinal criptografado ter uma distribuição de potência própria que pode excitar ainda mais as não-linearidades do sistema, esses sinais ainda podem ser propagados por redes metropolitanas com diâmetros maiores que 640 km. Isso indica o potencial de utilização da técnica em sistemas comerciais de comunicação óptica. Adicionalmente, mostramos que trabalhar com uma abordagem de chaves dinâmicas torna a DSP-SPE-Scr ainda mais segura porque, com essa abordagem, as propriedades de difusão e confusão de Shannon e a segurança semântica são satisfeitas. No melhor de nosso conhecimento, essa é a primeira vez que chaves dinâmicas são aplicadas a algoritmos de encriptação de sinais, com a avaliação das propriedades de difusão, confusão e segurança semântica.

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

Abstract

SANTOS, Melissa de Oliveira. **Encryption in the Physical Layer Based on Spectral Encoding Implemented by DSP and Applied to Optical Networks.** 2020. 65 p. Dissertation (Master of Electrical Engineering) – Campus São João da Boa Vista, São Paulo State University, São João da Boa Vista, 2019.

The objective of this project is to propose and evaluate the application of a new signal encryption technique for optical communications systems. The technique consists of using digital signal processing to: i) divide an input signal into several spectral slices, ii) apply a own phase shift to each slice, iii) to scramble these slices and iv) spectrally multiplex all slices, v) to generate a baseband output signal which is an encrypted (distorted) version of the input signal. This technique was called spectral phase encoding and scrambling cryptography by digital signal processing, DSP-SPE-Scr. The baseband encrypted signal is then modulated on an optical carrier and propagated by a transparent optical network. Results obtained suggest that the technique is safe against brute force attacks. Moreover, although the encrypted signal has a different power distribution that might excites the nonlinearities of the system, these signals can still be propagated by metropolitan networks with a diameter larger than 640 km, which indicates that the technique may be applied to commercial optical communication systems. Additionally, we found that working with the dynamic keys strategy in the DSP-SPE-Scr makes it even safer because, with this approach, Shannon's diffusion and confusion properties and semantic security are satisfied. To the best of our knowledge, this is the first time the dynamic keys are applied to signal encryption algorithm with the evaluation of diffusion and confusion properties and semantic security.

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

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

A	Ampere
AES	Padrão de criptografia avançada
AWGN	Ruído aditivo gaussiano e branco
BER	Taxa de erro de bit
BFA	Ataque de força bruta
BPSK	Modulação por deslocamento de fase binária
B2B	*Back-to-back*
dB	Decibel
DCF	Fibra compensadora de dispersão
DSP	Processamento digital de sinais
DSP-SPE	Criptografia de codificação espectral de fase por processamento digital de sinais
DSP-SPE-Scr	Criptografia de codificação espectral de fase e embaralhamento intra-canal por processamento digital de sinais
D/A	Conversor digital-analógico
EDFA	Amplificador de fibra dopada com érbio
EVM	Vetor de magnitude de erro
F	Distância focal
FEC	Correção de erros a frente
FFT	Transformada rápida de Fourier
GBaud	Giga Baud
Gbps	Giga bits por segundo

GHz	Giga Hertz
GVD	Dispersão de velocidade de grupo
G1	Ganho do amplificador 1
G2	Ganho do amplificador 2
Hz	Hertz
I	Componente em fase do sinal
IFFT	Transformada inversa rápida de Fourier
ISI	Interferência intersimbólica
km	Kilometro
OFDM	Multiplexação por divisão de frequências ortogonais
OSI	Interconexão de sistemas abertos
OSNR	Razão sinal-ruído óptica
PAM	Modulação por amplitude de pulso
PMD	Dispersão de modo de polarização
PONs	Redes ópticas passivas
PRBS	Sequência pseudoaleatória de bits
P/S	Conversor paralelo-série
Q	Componente em quadratura do sinal
QAM	Modulação de amplitude em quadratura
QKD	Distribuição de chave quântica
QPSK	Modulação por deslocamento de fase em quadratura
RCF	Filtro cosseno-levantado
S	Inclinação da dispersão

SER	Taxa de erro de símbolo
SLM	Modulador espacial de luz
SNR	Razão sinal-ruído
SPDE	Codificação espectral de fase e atraso
SPE	Codificação espectral de fase
SPM	Automodulação de fase
SSMF	Fibra monomodo padrão
S/P	Conversor série-paralelo
TON	Rede óptica transparente
W	Watt
WDM	Multiplexação por divisão de comprimento de onda
XOR	Ou-Exclusivo

Lista de símbolos

n_s	Número de fatias
m_1	Sinal complexo de entrada
n_{sa}	Número de amostras
t	Tempo
n	Número inteiro
T_s	Período de símbolo
f	Frequência
k_c	Chave criptográfica para a operação de codificação de fase
ϕ	Fase adicionada às fatias
k_e	Chave criptográfica para a operação de embaralhamento intracanal
c_1	Sinal complexo criptografado no domínio eletrônico
f_{c1}	Frequência da portadora
e_1	Sinal ópitco criptografado
e_1'	Sinal ópitco criptografado após a propagação
c_1'	Sinal complexo criptografado no domínio eletrônico após a propagação
m_1'	Sinal de entrada recuperado com uma certa penalidade
K_t	Chave temporária
K_i	Chave inicial
K_s	Chave semente
DK	Chave dinâmica
R_s	Taxa de símbolo
B	Banda do sinal

r	Fator de decaimento do filtro
$P(C)$	Probabilidade de acerto de símbolo
M	Número de símbolos
$P(C\|m_j)$	Probabilidade condicional de acerto de símbolo dado que o símbolo m_j foi transmitido
$P(m_j)$	Probabilidade de m_j ser transmitido
P_{eM}	Probabilidade de erro de símbolo
P_{eB}	Probabilidade de erro de bit
d	Distância de separação entre símbolos
σ_N	Desvio padrão de ruído
E_b	Energia do bit
$\aleph$	Densidade espectral de potência do ruído
E	Energia média
P	Potência média
σ^2	Variância de uma variável aleatória com distribuição gaussiana
σ_x^2	Variância associada ao eixo I da gaussiana
σ_y^2	Variância associada ao eixo Q da gaussiana
σ	Desvio padrão da gaussiana
G_{dB}	Ganho em decibéis
α	Atenuação
L	Comprimento da fibra
$\Delta\theta$	Erro ou diferença média da fase
θ_i	Fase da i-ésima fatia

$\theta_{intruso,i}$	Fase adotada por um intruso na i-ésima fatia
$\Delta\theta_{max}$	Máximo erro permitido na fase para recuperar o sinal
n_t	Número de tentativas
β	Constante de propagação
f_0	Frequência central
β_0	Coeficiente linear
β_1	Parâmetro de dispersão de primeira ordem
β_2	Coeficiente de velocidade de grupo
β_3	Parâmetro de dispersão de terceira ordem

Sumário

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

1 Introdução

A segurança de uma rede é um dos itens de projeto mais discutidos atualmente. Isso porque as brechas de segurança de rede, além de degradarem a imagem da prestadora de serviço, ainda acarretam muitos prejuízos.

Criptografia é o meio mais utilizado para garantir a confidencialidade da rede, sendo a confidencialidade um dos principais atributos para garantir a segurança. Contudo, para conseguir uma técnica de criptografia realmente eficiente, é necessário seguir alguns princípios básicos. A primeira seção desse capítulo é dedicada à discussão de alguns desses princípios. A Seção 2 exibe à revisão bibliográfica das técnicas de criptografia para sinais ópticos, seguida da seção com as principais contribuições do trabalho. A última seção desse capítulo descreve a organização da dissertação.

1.1 Princípios de Criptografia

Em 1945, Shannon escreveu um artigo nomeado *A Mathematical Theory of Cryptography*, publicado em uma versão mais curta em 1949 (Shannon, 1949). Nesse artigo, Shannon descreve duas propriedades de operação que, se satisfeitas em uma cifra, a qualifica como segura. Isso porque, quando presentes, impedem a aplicação de estatísticas e outros métodos para solucionar a criptografia aplicada.

A primeira propriedade é chamada de difusão. Basicamente, o que essa propriedade requer é que, se alterarmos os dados da mensagem de entrada em apenas um bit, os dados da mensagem criptografada devem variar em aproximadamente 50% dos bits. Isso comprova a não existência de nenhuma relação entre a mensagem de entrada e a mensagem criptografada e dificulta a ação do intruso (*eavesdropper*) de descobrir a mensagem original.

A segunda propriedade, conhecida como confusão, requer que cada bit da mensagem criptografada dependa de muitos bits da chave criptográfica e que a relação entre as duas não seja intuitiva. Ou seja, a confusão serve para ocultar a relação entre cifra e chave. Essa propriedade pode ser conferida da seguinte maneira: se um bit da chave criptográfica for alterado, muitos bits da mensagem criptografada também devem ser alterados. De maneira mais rigorosa, podemos seguir a lógica da difusão e estabelecer que aproximadamente 50% dos bits da mensagem criptografada devem ser alterados para garantir confusão.

Um outro princípio de criptografia bastante importante é o de segurança semântica. Para garantir que um esquema de criptografia seja semanticamente seguro, não se pode obter nenhuma informação dos dados criptografados que estão sendo transmitidos. Portanto, se vários blocos de dados criptografados estão sendo transmitidos, todos devem ser diferentes uns dos outros, mesmo que não haja nenhuma alteração entre eles.

Esses princípios levaram em consideração o único tipo de criptografia existente na época: a criptografia de dados. Essa criptografia, que age sobre os bits que estão armazenados em nossos computadores, já é muito bem estabelecida e utilizada em sistemas de comunicações práticos. Como exemplo de criptografia de dados têm-se o *Advanced Encryption Standard* (AES) com chaves criptográficas de 128, 192 ou 256 bits, padrão mais utilizado atualmente (Fips, 2009). Porém, ao considerar a transmissão por uma rede, esses bits são, eventualmente, convertidos em sinais que também podem ser criptografados. Por esse motivo, atualmente lidamos com um segundo tipo de criptografia que ainda é um tópico de pesquisa e não tem sido aplicada comercialmente até o momento: a criptografia de sinais. Esse processo ocorre na camada física do modelo para interconexão de sistemas abertos (*open system for interconnections*, OSI), por isso é comumente referenciado como criptografia de camada física, assim como aparece no título deste trabalho.

A motivação para estudar a criptografia de sinais é que ela apresenta pelo menos duas vantagens sobre a criptografia de dados. Primeiro, sendo essa criptografia aplicada na camada física, ela também criptografa os dados de todas as camadas superiores do modelo OSI. Além disso, adicionar uma proteção ao sinal enquanto ele está sendo propagado pela rede é muito importante, visto que, usualmente, os donos da rede não são os mesmos a quem a informação que está trafegando nela pertencem.

Adicionalmente, assim como as redes de comunicações sem fio, as redes ópticas também estão sujeitas à espionagem, devido à existência de mecanismos intrusivos e não-intrusivos para derivar (*tap*) sinais de redes ópticas (Iqbal; Fathallah; Belhadj, 2011; Peng *et al.*, 2011; Shaneman; Gray, 2004). Essa situação tem motivado o estudo de técnicas que fornecem segurança na camada física desses sistemas (Dahan; Mahlab, 2017). Na seção a seguir, abordaremos algumas dessas técnicas.

1.2 Revisão bibliográfica

A criptografia de sinais vem sendo um alvo muito intenso de pesquisas acadêmicas. Por diversos fatores que serão abordados nessa seção, no melhor do nosso conhecimento, essas técnicas ainda não são implementadas em sistemas comerciais com intuito de aumentar a segurança. É por isso que nesse trabalho há uma preocupação em conseguir atender as demandas de redes metropolitanas comerciais.

1.2.1 Criptografia óptica aplicada em sinais ópticos

Podemos encontrar na literatura algumas técnicas de criptografia aplicadas a sinais modulados em portadoras ópticas. Dentre essas técnicas, de fato, a maneira mais segura de criptografar sinais é utilizando alguma abordagem quântica. Criptografia quântica é bastante promissora no ponto de vista de segurança, visto que ajuda a identificar quando há alguém malicioso agindo. No entanto, sua utilização para criptografar sinais em redes ópticas comerciais que utilizam a tecnologia de multiplexação por divisão em comprimento de onda (*wavelength division multiplexing*, WDM) ainda não é prática. A taxa de transmissão de sinais criptografados quanticamente é bastante inferior às usadas em redes comerciais, devido à redundância de informação que a técnica necessita para uma recepção eficiente (Moizuddin; Winston; Qayyum, 2017). Atualmente é possível encontrar na literatura alguns protocolos de criptografia quântica com taxas de transmissão razoáveis, porém esses protocolos se abrem para uma fraqueza a um perigo maior: o de ataque de canal lateral, do inglês *side-channel attack* (Pirandola *et al.*, 2019). Esse ataque refere-se às informações que podem ser obtidas ao fazer a implementação da técnica. Essas informações podem estar relacionadas ao tempo, consumo de energia, som, entre outros.

Uma outra possibilidade é a utilização da criptografia caótica (Gayathri; Subashini, 2016; Wei *et al.*, 2019). Apesar de importantes avanços na sincronização requerida para o bom funcionamento de sistemas caóticos (Pecora; Carroll, 1990; Pecora; Carroll, 2015; Pizolato; Romero; Neto, 2008), os sistemas atuais baseados nessa tecnologia ainda operam com taxas da ordem de 10 Gbps (Zhao *et al.*, 2020; Zhao *et al.*, 2019) que são consideravelmente menores àquelas usadas nos sistemas WDM atuais.

A técnica baseada na utilização de portas ópticas responsáveis por fazer as operações da função lógica ou-exclusivo (*exclusive or*, XOR) também é mais uma possibilidade estudada para criptografia na camada física. A aplicação dessa técnica é vantajosa por operar em alta velocidade, como o sistema de 120 Gbps descrito em (Agarwal; Pareek; Agarwal, 2018). Porém, os dispositivos necessários para sua aplicação utilizam-se de efeitos não-lineares, o que dificulta bastante a implementação prática (Dahan; Mahlab, 2017).

Por último, podemos citar a técnica de criptografia baseada em codificação espectral. Por essa ser a criptografia de referência para a técnica desenvolvida nesse trabalho, faremos uma descrição mais detalhada dessa técnica na próxima subseção.

1.2.2 Criptografia óptica baseada em codificação espectral

Essa subseção se dedica a explicar como funciona a estratégia de criptografia de sinais ópticos baseada em codificação espectral. Nessa estratégia, o sinal óptico é dividido em diversas fatias espectrais e então alguma técnica é aplicada nessas fatias para distorcer o sinal a ser propagado. Duas das primeiras técnicas que vieram dessa estratégia alteram alguma propriedade das fatias espectrais: se a propriedade alterada for a fase da fatia, a técnica é referenciada como codificação espectral de fase (*spectral phase encoding*, SPE) (Cornejo; Tocnaye, 2008), caso tivermos tanto uma mudança de fase quanto a aplicação de um atraso em cada fatia, a técnica é chamada de codificação espectral de fase e de atraso (*spectral phase and delay encoding*, SPDE) (Abbade *et al.*,). Outra técnica que veio em seguida realiza um embaralhamento entre as fatias de dois, ou até mais, sinais distintos. Essa técnica também é um trabalho do nosso grupo de pesquisa e é chamada de embaralhamento intercanal (*shuffling*) (de Andrade Bragagnolle *et al.*, 2019; Santos *et al.*, 2019). A seguir, explica-se a SPE, que é uma das técnicas que motivou a realização desse trabalho.

A Fig. 1 ilustra um diagrama de blocos para a SPE. Um sinal é dividido em n_s fatias ópticas e cada uma dessas fatias recebe sua própria fase. As fatias são então multiplexadas e formam um novo sinal com a mesma banda do sinal original, mas esse novo sinal está criptografado devido à distorção causada pelos desvios de fase adicionados a cada uma das fatias. A chave criptográfica desse sistema é formada pelo conjunto desses desvios. Após ser propagado por uma rede óptica, o sinal criptografado chega ao nó receptor autorizado

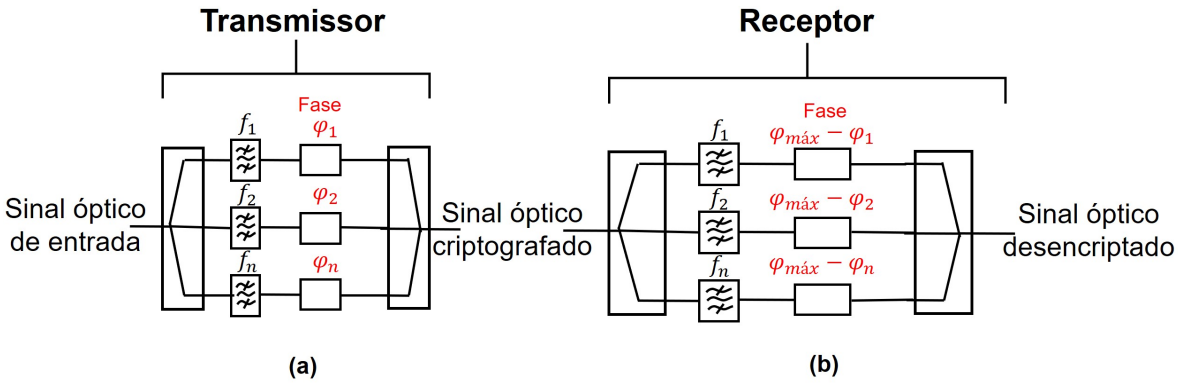

Figura 1 – Representação dos processos de encriptação (a) e desencriptação (b) de um sinal óptico por SPE.

onde a chave criptográfica é conhecida. A chave pode ser trocada entre transmissor e receptor por distribuição de chave quântica (*quantum key distribution*, QKD) via satélites (Liao *et al.*, 2017), conduzindo a uma abordagem toda de camada física. Possuindo a chave do sistema, para remover a criptografia, o receptor precisa dividir o sinal criptografado nas mesmas fatias anteriores e aplicar a cada uma delas um desvio de fase complementar àquele usado na encriptação. Assim, após uma nova multiplexação das fatias espectrais, o sinal original é recuperado com uma certa penalidade de propagação.

Entre todas as estratégias apresentadas na Subseção 1.2.1, as técnicas de criptografia de sinais ópticos que são baseadas em codificação espectral são as que melhor se adaptam às situações de redes ópticas comerciais. Nessas técnicas, a banda do sinal criptografado é a mesma do sinal original e isso garante compatibilidade com sistemas WDM. Além disso, as taxas de transmissão podem ser as mesmas usadas nas redes comerciais e resultados de simulações sugerem que o alcance dos sinais transmitidos pode ser superior a algumas centenas de quilômetros mesmo para sinais com modulação de amplitude em quadratura (*quadrature amplitude modulation*, QAM) com 16 símbolos distintos (16-QAM) com taxa igual a 200 Gbps (Abbade *et al.*,).

Por outro lado, surge uma dificuldade para realizar essas técnicas de maneira totalmente óptica. Isso porque é muito complicado obter fatias com banda estreita. Uma primeira maneira seria criar essas fatias por meio de filtros ópticos. Assim, por exemplo, se for necessário dividir um sinal com uma banda típica de 50 GHz em 10 fatias espectrais, precisaremos de filtros ópticos com uma largura de banda de 5 GHz. Embora a literatura aponte a possibilidade de fabricação de filtros com bandas até mesmo inferiores a 1 GHz

(Chen *et al.*, 2010; Zou *et al.*, 2013), esses dispositivos não estão disponíveis comercialmente e isso dificulta a investigação prática do desempenho da técnica.

Outra possibilidade é a utilização do esquema de encriptação 4F considerado em (Cornejo; Tocnaye, 2008) para o caso da SPE e também em (Santos *et al.*, 2019) para uma técnica de *shuffling*. Esse esquema utiliza de um módulo de seleção de fatias composto por cinco elementos separados por uma distância focal F dos elementos adjacentes, por isso o nome 4F. Porém, assim como as outras técnicas, essa também possui desvantagens que podem afetar o desempenho do processo de encriptação e a implementação prática. Uma dessas desvantagens está relacionada com o modulador espacial de luz (*spatial light modulator*, SLM), que pode apresentar certa interferência entre as fatias adjacentes, causando uma certa degradação na recepção do sinal, como explicado em (Santos *et al.*, 2019).

Uma maneira de superar as limitações dos dispositivos ópticos é realizar o processo de criptografia no sinal em banda-base, como observa-se na subseção a seguir.

1.2.3 Criptografia óptica aplicada em sinais em banda-base

Essas dificuldades mencionadas na subseção anterior estão, em grande parte, relacionadas ao fato de dispositivos ópticos serem tradicionalmente fabricados com o intuito de transmitir, receber e/ou comutar sinais, mas de não estarem adaptados para realizar, de maneira eficiente, funções de processamento óptico de sinais, como as necessárias para criptografar sinais.

Sendo assim, é justificável o desejo por realizar a criptografia de sinais que trafegam em sistemas de comunicações ópticas no domínio eletrônico. Seguindo essa estratégia, pode-se aplicar a criptografia ao sinal em banda-base e, para esses sinais trafegarem por redes ópticas, basta que, posteriormente, esses sejam convertidos para o domínio óptico em algum processo de modulação óptica. Em especial, se a criptografia for feita por meio de processamento digital de sinais (*digital signal processing*, DSP), os códigos desenvolvidos para a criptografia de sinais poderão ser facilmente replicados de um equipamento para outro. Esse benefício apresenta uma grande vantagem para as operadoras interessadas na técnica, pois diminuirá o custo de implementação.

Algumas das técnicas citadas na Subseção 1.2.2 já foram aplicadas no domínio digital e constam na literatura. Por exemplo, a técnica SPDE (Abbade *et al.*, 2018) e a técnica de embaralhamento intercanal (Abbade *et al.*, 2020). A flexibilidade de se usar processamento digital de sinal permite algumas operações que não eram possíveis de serem feitas no domínio óptico. Como exemplo temos uma operação bastante útil, que era utilizada em criptografia de dados e que está sendo transferida para criptografia de sinais, que é trocar as unidades de informação de posição. Essa operação para criptografia de sinais é utilizada nesse trabalho e é chamada de embaralhamento intracanal (*scrambling*). Seu funcionamento estará descrito no Capítulo 2.

Além disso, o uso de DSP facilita a implementação de chaves criptográficas que possibilitam alcançar as propriedades de difusão e confusão de Shannon e a segurança semântica. Como exemplo, temos (Zhang *et al.*, 2017), que utiliza uma chave obtida a partir de uma estratégia de caos para sinais com multiplexação por divisão de frequências ortogonais (*orthogonal frequency division multiplexing*, OFDM). Os resultados desse trabalho e de vários outros do mesmo grupo são experimentais e aplicam-se a redes ópticas passivas (*passive optical networks*, PONs). No melhor de nosso conhecimento, no entanto, não há trabalhos similares aplicados a sinais de portadora única que se propagam por redes de maior alcance.

Tendo em vista essa lacuna e que a grande maioria dos sistemas comerciais de comunicações ópticas da atualidade emprega sinais de portadora única, o objetivo desse trabalho é avaliar uma nova técnica de criptografia para criptografar, no domínio digital, esses sinais. Essa nova técnica combina as operações das técnicas SPE e de embaralhamento intracanal e é referenciada como DSP-SPE-Scr.

1.3 Contribuições

Esse trabalho apresenta algumas contribuições que serão detalhadas a seguir. Em primeiro, desenvolveu-se e testou-se um código para avaliar a realização da SPE e da SPDE em DSP. Em conjunto, foi adicionado ao código a operação de embaralhamento intracanal que conclui a nova técnica proposta nesse trabalho. Esses códigos foram incluídos ao *software* KryptoSJ que também foi utilizado para aplicação de outras técnicas de criptografia dentro do nosso grupo de pesquisa (Nogueira; Abbade, 2019; Souza; Abbade, 2019).

Do ponto de vista técnico, as principais contribuições desses resultados são: i) a avaliação da robustez da nova técnica DSP-SPE-Scr em relação a ataques de força bruta (*brute force attacks*, BFAs) e ii) testes referentes à difusão, confusão e segurança semântica em casos que chaves dinâmicas (Ngo *et al.*, 2010) são aplicadas à DSP-SPE-Scr.

Além da pesquisa acerca da técnica proposta nesse trabalho, a autora também participou ativamente dos novos trabalhos do grupo, em relação às novas técnicas de criptografia, e isso resultou em uma boa produção científica. Sendo três publicações em congressos (Abbade *et al.*, 2018; de Andrade Bragagnolle *et al.*, 2019; Santos *et al.*, 2019) e uma publicação em *journal* (Abbade *et al.*, 2020). Além disso, existem dois artigos submetidos para eventos científicos, ambos como trabalhos convidados (Abbade *et al.*, Submetido em abril de 2020; Souza *et al.*, Submetido em abril de 2020).

Por fim, nota-se que o trabalho foi elaborado pensando-se em aplicações comerciais e pode ser de interesse para operadoras, bancos, grandes empresas que precisam de um elevado nível de confidencialidade em suas comunicações, setor militar e, também, para instituições governamentais.

1.4 Organização do trabalho

O restante dessa dissertação está organizado da maneira que se segue. No Capítulo 2 a autora descreve teoricamente como são os mecanismos de criptografia utilizados no trabalho, como as operações de codificação de fase e de embaralhamento intracanal e a técnica de chaves dinâmicas. O Capítulo 3 traz a lógica do *software* KryptoSJ que foi desenvolvido para a aplicação dessa técnica, juntamente com os códigos adicionados para ajudarem na captura e análise de resultados. No Capítulo 4 encontra-se a descrição do cenário de simulação em relação ao *software* VPITransmissionMaker que foi utilizado para obter os resultados. Esse mesmo capítulo também contém todos os resultados e as discussões acerca da técnica e sua aplicabilidade. Os resultados nesse capítulo são separados em seis subseções. A primeira subseção analisa o quão segura é a técnica em relação a BFA. A segunda e a terceira subseção discute a penalidade sofrida pelo sinal criptografado em banda-base e após passar pelo processo de modulação óptica, respectivamente. A quarta subseção estende a análise anterior para quando o sinal é propagado por uma rede óptica. A quinta subseção dedica-se à análise sobre as propriedades de difusão e confusão e à

segurança semântica advindas da aplicação de chaves dinâmicas. A última subseção faz menção aos testes experimentais realizados no CPqD. Finalmente, a conclusão obtida com esse trabalho e uma lista de publicações e prêmios alcançados pela autora são apresentados no Capítulo 5.

2 Descrição dos mecanismos de criptografia

Como mencionado no Capítulo 1, o propósito desse trabalho é implementar códigos para analisar uma técnica que inclui as operações utilizadas nas técnicas SPE e de embaralhamento intracanal. Essa técnica será desenvolvida com processamento digital de sinais, sendo aplicada a sinais em banda-base. O nome escolhido para referenciá-la é DSP-SPE-Scr.

2.1 Descrição da DSP-SPE-Scr

A Fig. 2 apresenta um diagrama de blocos relativo às principais operações da DSP-SPE-Scr. Um sinal complexo $m_1[k]$ com componentes referentes aos eixos I e Q, é amostrado e processado por um conversor série-paralelo (S/P) que agrupa as amostras desse sinal em sequências de n_{sa} amostras. Depois, um algoritmo de transformada rápida de Fourier (*fast Fourier transform*, FFT) é usado para converter esse sinal para o domínio da frequência e, a seguir, processá-lo por um filtro de Nyquist, que no caso desse trabalho foi um filtro cosseno levantado (*raised-cosine filter*. RCF),

Originalmente, filtros de Nyquist são usados para prover proteção contra interferência intersimbólica (*intersymbol interference*, ISI) (Lathi; Ding, 2012). Em particular o cosseno levantado é uma função com amplitude não nula em $t = 0$ e amplitudes nulas em $t = \pm nT_S$ em que t é o tempo, n é um número inteiro e T_S é o período de símbolo, como mostra a Fig. 3. Essa figura deixa claro que as amostras em t =0, T_S, $2T_S$, $3T_S$... consistem

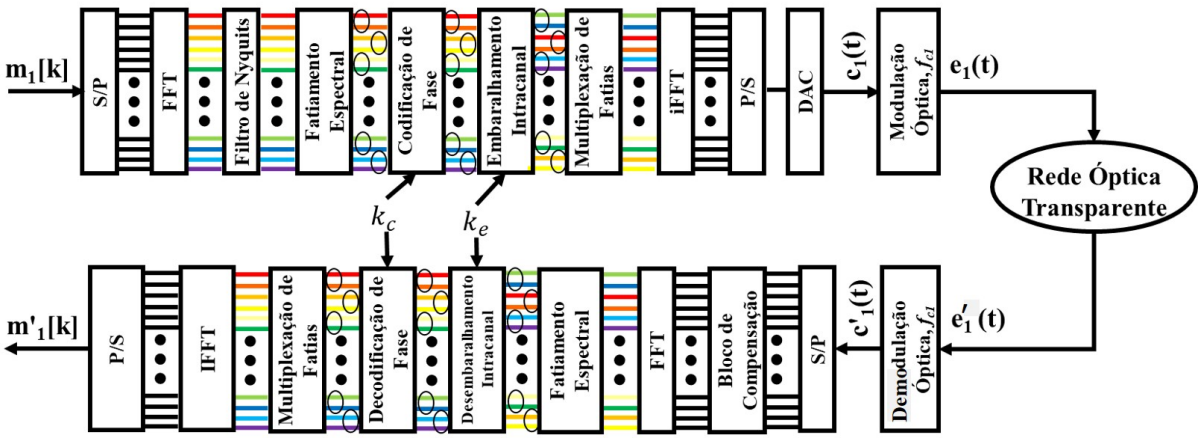

Figura 2 – Diagrama de blocos para a técnica DSP-SPD-Scr aplicada a uma rede óptica.

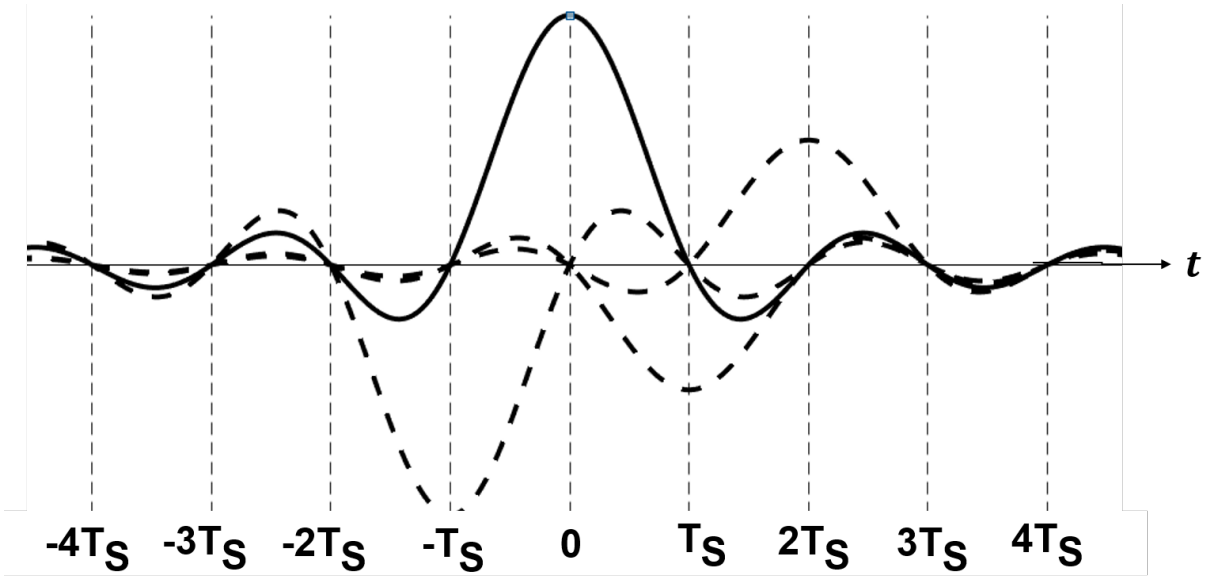

Figura 3 – Símbolos cosseno levantado satisfazendo os critérios de Nyquist para ISI nula.

na amplitude de apenas um pulso, sem nenhuma interferência de outros. Porém, para isso ser válido, o sinal deve chegar ao receptor com esse formato. No entanto, em comunicações ópticas, como visto na Fig. 2, é usual utilizar o filtro de Nyquist no transmissor para limitar a banda do sinal. Assim, o pulso não chega com o formato necessário ao receptor e, com a dispersão da fibra, teremos ISI que pode ser compensada opticamente ou por meio de DSP (Agrawal, 2014). No segundo desses casos, é relativamente fácil determinar uma função de transferência que compense as distorções conjuntas causadas pelo filtro de Nyquist e pela fibra, compensando a ISI e atendendo ao critério de Nyquist para ISI nula.

Uma outra função adicional do RCF será detalhada a seguir. Se os símbolos relacionados ao sinal na entrada são representados por símbolos retangulares ($rect(\frac{t}{T_S})$), então o espectro de Fourier desse sinal terá uma forma proporcional a uma função *sinc* ($T_S sinc(\pi f T_S)$), em que f é a frequência de cada componente espectral do sinal (Lathi; Ding, 2012). Assim, algumas componentes espectrais apresentam uma amplitude naturalmente maior que outras. Em um ataque, essa característica permite que um intruso possa priorizar a descoberta das componentes de frequência (fatias) que têm maior amplitude para descobrir o conteúdo do sinal. Por outro lado, a transmissão de um sinal por um filtro RCF faz com que o espectro de Fourier do sinal torne-se mais plano. Dessa forma, no caso de um ataque, as fatias centrais terão uma amplitude similar e o intruso terá que decodificar um número maior delas para recuperar o conteúdo do sinal com certa taxa de erro bit (*bit error rate*, BER).

Voltando ao diagrama de blocos da Fig. 2, o sinal na saída do filtro é, então, dividido em n_s fatias espectrais, cada uma com n_{sa}/n_s amostras. Após isso, as fatias são codificadas de acordo com uma chave que é aleatoriamente gerada k_c. Essa chave é composta por um conjunto de fases ϕ. Esse processo é realizado pela multiplicação do sinal associado a cada fatia por $e^{j\phi}$. No próximo passo, ocorre o embaralhamento intracanal. Nesse bloco, ocorre uma permutação entre as fatias espectrais do sinal de acordo com uma segunda chave k_e que também é gerada aleatoriamente. A chave k_e é composta de duas colunas, em que a primeira mostra a posição inicial de cada fatia e a segunda coluna especifica qual posição a fatia deve ocupar com a operação de embaralhamento. Após isso, as fatias são multiplexadas espectralmente. O sinal resultante é então submetido a uma FFT inversa (IFFT) que o converte para o domínio temporal. Um conversor paralelo-série (P/S) serializa as amostras do sinal e as envia para um conversor digital-analógico (D/A), cuja saída $c_1(t)$ corresponde às componentes complexas do sinal em banda-base criptografado.

O sinal encriptado pela DSP-SPE-Scr, de acordo com as operações explicadas anteriormente, é submetido a uma modulação óptica com uma dada frequência de portadora f_{c1} e convertido ao domínio óptico. O sinal óptico resultante $e_1(t)$ é, então, propagado por uma rede óptica transparente (*transparent optical network*, TON), até o seu destino. O sinal $e_1'(t)$, que chega ao receptor conhecido, é demodulado com a mesma frequência portadora da modulação f_{c1}, resultando no sinal complexo em banda-base $c_1'(t)$.

O mecanismo para desencriptar o sinal vem em seguida e envolve os passos "complementares" aos usados no processo de encriptação: a paralelização do sinal para agrupá-lo em amostras seguido de um bloco que pode compensar de maneira digital penalidades causadas pela dispersão cromática, dispersão de modo de polarização (*polarization mode dipersion*, PMD), ruído de fase e efeitos não-lineares introduzidos pelo modulador, fibra e receptor. Esse mesmo bloco também é dedicado para fazer a sincronização entre transmissor-receptor. Depois, o sinal é mandado para um algoritmo de FFT para passá-lo ao domínio da frequência e permitir separar o sinal em n_s fatias espectrais. Com o acesso às chaves do sistema, o decodificador reorganiza as fatias na ordem inicial e as multiplicam pela exponencial complexa $e^{-j(\phi)}$ enviando-as para um multiplexador espectral. O processo de IFFT e serialização finaliza a técnica e resulta no sinal $m_1'[k]$. Esse sinal representa a recuperação do sinal de entrada com uma certa penalidade.

Um mecanismo eficiente de encriptação na camada física deve fazer com que os sinais criptografados tenham uma BER elevada e deve satisfazer os princípios de criptografia que

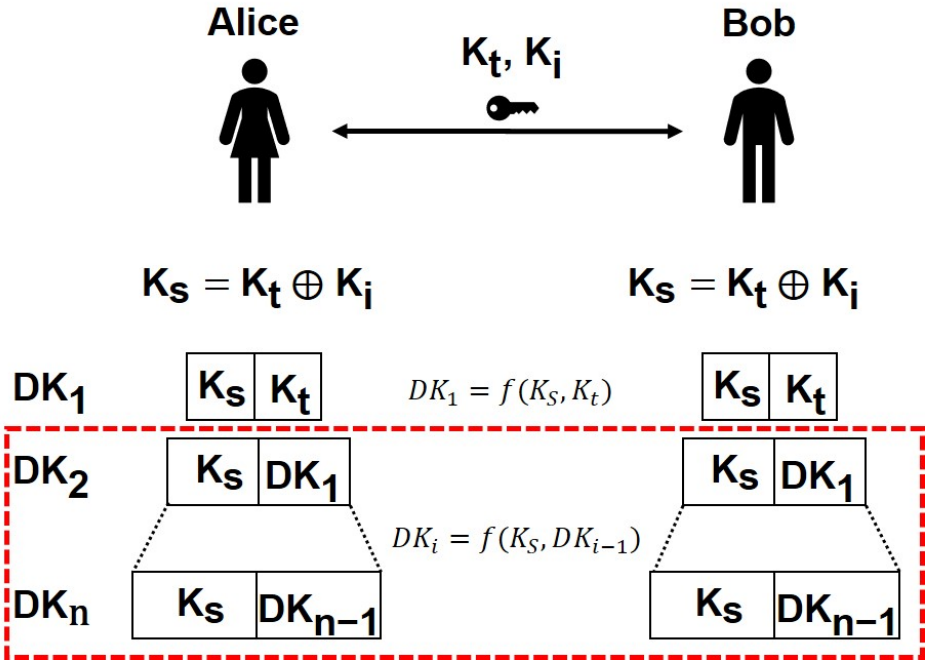

Figura 4 – Esquemático simplificado da geração de chaves dinâmicas

foram mencionados no Capítulo 1. Como será mostrado em nossos resultados, a estratégia empregada oferece uma BER elevada, mas não atende as propriedades de Shannon e a segurança semântica. Para resolver esse problema foi necessário implantar uma estratégia em que a chave de encriptação varia dinamicamente entre um bloco e outro. Essa estratégia é descrita na seção a seguir.

2.2 Descrição de chaves dinâmicas

A explicação completa acerca de chaves dinâmicas pode ser encontrada em (Ngo *et al.*, 2010). A Fig. 4 ilustra uma explicação simplificada, que foi adaptada para a solução do problema desse trabalho, acerca da geração da chave dinâmica, que segue três passos:

1. Primeiro, há uma troca de chaves entre Alice e Bob que pode ser feito como mencionado na Subseção 1.2.2. Essas chaves são a chave temporária K_t e a chave inicial K_i
2. No segundo passo, tanto Alice quanto Bob vão gerar uma mesma chave semente K_s que será uma função XOR entre as chaves trocadas inicialmente:

$$K_s = K_t \oplus K_i \tag{1}$$

3. No terceiro passo, começa a geração das chaves dinâmicas. Para conseguir DK_1, Alice aplica de uma função de mão-única à K_s e K_t:

$$DK_1 = f(K_s, K_t) \tag{2}$$

A função de mão-única é uma função especial que tem fácil aplicação no sentido direto, enquanto é relativamente difícil e demorado calcular o inverso. Portanto, Alice começa a criar uma chave que apenas ela e Bob conseguem, de fato, calcular. Nesse trabalho, a função inversa aplicada foi a função de *whirlpool*. O cálculo das chaves dinâmicas que se seguem (DK_2, DK_3, ..., DK_n), em que n é um número inteiro muito elevado, são feitos a partir da aplicação da função de *whirlpool* entre a chave semente e a chave dinâmica anterior:

$$DK_i = f(K_s, DK_{(i-1)}) \tag{3}$$

Utilizando a técnica de chaves dinâmicas, conseguimos que a chave de um bloco seja sempre diferente da chave que foi utilizada no bloco anterior. Com isso, é possível satisfazer as propriedades de difusão e confusão de Shannon, além da segurança semântica.

3 *Software* desenvolvido

Toda a lógica usada para o desenvolvimento do *software* que será apresentado nesse capítulo foi implementada com a linguagem de programação Matlab®.

É importante ressaltar que o grupo de pesquisa ao qual esse trabalho está inserido já havia começado o desenvolvimento de um *software*, que foi nomeado como KryptoSJ. Antes das alterações da autora, esse *software* criptografava sinais com modulação por amplitude de pulso (*pulse-amplitude modulation*, PAM) de 2 símbolos, 2-PAM real, segundo a SPE ou SPDE com DSP e gerava alguns gráficos para análise. Esses sinais após modularem uma portadora óptica, originam sinais com modulação por chaveamento de desvio de fase binária (*binary phase-shift keying*, BPSK). Agora, o código que aplica a DSP-SPE-Scr em sinais multiníveis 2-PAM e 4-PAM complexos, que quando modulados geram sinais com modulação por deslocamento de fase em quadratura (*quadrature phase shift keying*, QPSK) e 16-QAM respectivamente, foi desenvolvido e incorporado ao KryptoSJ, juntamente com outras ferramentas de análises de desempenho que serão apresentadas e discutidas a seguir.

Nesse trabalho, chamaremos o sinal real 2-PAM de sinal BPSK em banda base. O sinal complexo composto por uma componente real 2-PAM e por uma componente imaginária 2-PAM será chamado de QPSK em banda base. De maneira análoga, o sinal complexo composto por componentes real e imaginária 4-PAM será denominado de 16-QAM em banda base.

O esquemático geral do KryptoSJ com as devidas modificações é apresentado na Fig. 5. A figura indica que existem três supermódulos: o "Transmissor", o "Receptor" e o "Estimador de BER" que podem ser executados independentemente, contanto que estejam alimentados. Cada um desses supermódulos contém seus próprios módulos, que necessitam do supermódulo para serem executados. O arquivo "Parâmetros de Entrada" alimenta os supermódulos "Transmissor" e "Receptor" (e, consequentemente, o "Estimador de BER") e contém todas as informações que são determinadas pelo usuário, sendo elas:

- Taxa de símbolos, R_s;
- Número de símbolos;
- Número de amostras por símbolo;
- Número de amostras por fatia, n_{sa};
- Fator de decaimento do filtro (*roll-off*);

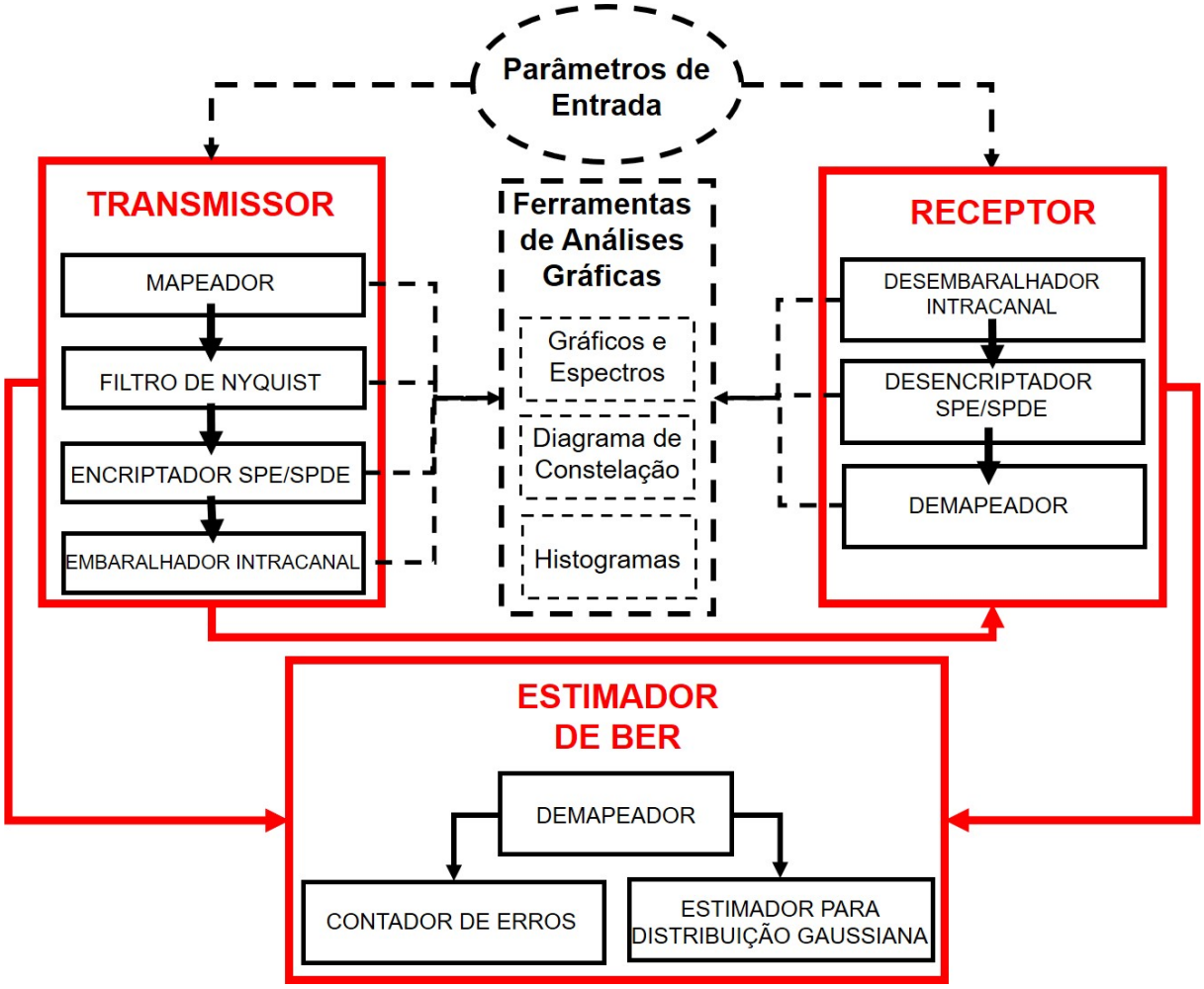

Figura 5 – Esquemático geral do funcionamento do *software* KryptoSJ

- Tipo de sinalização.

A partir desses parâmetros com entrada livre para o usuário, o arquivo "Parâmetros de Entrada" é capaz de calcular alguns outros parâmetros importantes para as simulações, como:

- Período de símbolo, T_s;
- Banda do sinal;
- Número de fatias espectrais, n_s, entre outros.

Sendo esse arquivo corretamente alimentado, os supermódulos podem ser executados. No supermódulo "Transmissor", o primeiro módulo "Mapeador" gera uma palavra pseudoaleatória de bits (*pseudo random bit sequence*, PRBS) e mapeia esses bits gerados em símbolos, associando-os aos eixos I e Q, de acordo com a sinalização informada pelo usuário em "Parâmetros de Entrada". Um vetor de tempo é definido a partir do período

de símbolo e do período de amostragem, também extraídos do arquivo "Parâmetros de Entrada" e é associado as amplitudes dos símbolos.

O sinal de saída do primeiro módulo passa então pelo "Filtro de Nyquist" que corresponde ao arquivo que simula um RCF, para limitar a banda do sinal. Após esse módulo o sinal fica contido em uma banda dada por:

$$B = \frac{R_s}{2}(1 + r) \tag{4}$$

em que R_s é a taxa de símbolo e r é o fator de decaimento (*roll-off*) do filtro, ambos extraídos do arquivo "Parâmetros de Entrada".

Depois de limitar a banda do sinal, o módulo "Encriptador SPE/SPDE" encarrega-se de realizar, no domínio da frequência, a criptografia que pode ser tanto a partir da técnica SPE quando SPDE, dependendo da escolha que o usuário faz no "Parâmetros de Entrada". O espectro será então dividido em n_s fatias espectrais. A seguir, para a técnica DSP-SPE-Scr, a partir de uma distribuição uniforme, os valores de fase ϕ_i são sorteados e aplicados a i-ésima fatia, conforme explicado no Capítulo 2. O conjunto dado pelos valores de ϕ_i compõe a primeira chave criptográfica do sistema, que fica armazenada em um documento a parte. Depois disso, passamos para a técnica de embaralhamento intracanal, em que as fatias são trocadas de posição de acordo com uma segunda chave. Essa chave é gerada por uma distribuição de *Bernoulli* com o número de elementos igual ao número de fatias. Antes de ir para a próxima etapa, as fatias do sinal são multiplexadas e voltam a compor um único vetor.

O supermódulo "Receptor" é responsável por fazer a desencriptação do sinal, ou seja, a recuperação do conteúdo do sinal. O primeiro módulo desse supermódulo tem acesso ao segundo documento em que a chave criptográfica da técnica de embaralhamento foi armazenada. Acessando o conteúdo desse documento ele é capaz de dividir o sinal em fatias novamente e voltá-las à posição inicial. Após isso, passamos para o módulo que irá remover a técnica de codificação de fase. Esse módulo tem acesso ao primeiro documento em que se encontra a primeira chave criptográfica criada. Fazendo o complemento do conteúdo desse documento e utilizando isso como chave para a remoção da criptografia, conforme explicado no Capítulo 2, é possível remover a criptografia SPE. Após isso, as matrizes serão enviadas ao módulo "Demapeador" para fazer o processo inverso do módulo "Mapeador", ou seja, para transformar as matrizes de amplitudes de símbolos em matrizes

de bits. O módulo "Demapeador" tem uma outra função adicional que será explicada juntamente com o supermódulo "Estimador de BER" a seguir.

O supermódulo "Estimador de BER" tem a função de retornar os valores de BER e de taxa de erro de símbolo (*symbol error rate*, SER) após o processo de criptografia (no "Transmissor") e após a remoção da mesma (no "Receptor"). Ou seja, o módulo estima a BER do sinal criptografado e do sinal recuperado. Uma outra métrica possível seria considerar o vetor de magnitude de erro (*error vector magnitude*, EVM) (Shafik; Rahman; Islam, 2006). No entanto, como nesse trabalho há um interesse em realizar comparações com o limite da correção antecipada de erros (*forward error correction*, FEC), e esse limite é expresso em termos da BER, optou-se por avaliar a BER. Portanto, para esse cálculo, dentro do supermódulo temos o mesmo módulo "Demapeador" do "Receptor". Esse módulo, além de fazer a conversão do sinal para uma matriz de bits, também aplicará a codificação Gray. O código Gray é aplicado para buscar transições de apenas um bit, de um símbolo adjacente para outro, em relação à constelação de um dado esquema de modulação. Esse procedimento vai ajudar a minimizar a BER. Feito isso, a saída do módulo "Demapeador" pode entrar em dois diferentes módulos, sendo eles o i) "Contador de Erros" e, ii) o "Estimador para Distribuição Gaussiana". O primeiro deles retorna a BER e a SER comparando as matrizes dos sinais criptografado (na saída do "Transmissor") e desencriptado (na saída do "Receptor"). Um erro é computado sempre que há uma diferença entre os elementos correspondentes dessas matrizes. Porém, essa técnica só pode ser usada em situações em que a magnitude da SER é suficientemente maior que o recíproco do número de símbolos simulados. Se essa condição não for satisfeita, pode ser que não se detecte nenhum bit errado ou, o número de bit errados detectados pode ser muito baixo e ser pouco confiável em termos estatísticos. Aumentar o número de símbolos simulados poderia ser uma solução, mas esse procedimento pode fazer com que as simulações fiquem muito lentas. Assim, para avaliar SERs menores que a da supracitada condição, utilizamos o cálculo pelo módulo "Estimador para Distribuição Gaussiana". Esse módulo estima a BER e a SER para um receptor de máxima verossimilhança (Lathi; Ding, 2012), sendo a probabilidade de acertos de símbolo dada por:

$$P(C) = \sum_{j=1}^{M} P(C|m_j)P(m_j) \tag{5}$$

em que M é o número de símbolos, $P(C|m_j)$ é a probabilidade condicional de acerto de símbolo dado que o símbolo m_j foi transmitido e $P(m_j)$ é a probabilidade de m_j ser transmitido. A partir dessa equação podemos calcular a probabilidade de erro de símbolo pela seguinte relação:

$$P_{eM} = 1 - P(C) \tag{6}$$

Por fim, depois do valor de P_{eM} ser conhecido, podemos calcular também a aproximação da probabilidade de erro de bit:

$$P_{eB} \approx \frac{P_{eM}}{log_2 M} \tag{7}$$

Supondo que o canal insira ruído aditivo, gaussiano e branco (*additive white Gaussian noise*, AWGN), as equações da SER para os sinais BPSK, QPSK e 16-QAM em banda-base ficam, respectivamente:

$$SER_{BPSK} = \frac{1}{2} erfc\left(\frac{d}{\sqrt{2}\sigma_N}\right) \tag{8}$$

$$SER_{QPSK} = erfc\left(\frac{d}{\sqrt{2}\sigma_N}\right) \tag{9}$$

$$SER_{16-QAM} = \frac{3}{2} erfc\left(\frac{d}{\sqrt{2}\sigma_N}\right) \tag{10}$$

em que $erfc$ é a função erro complementar, d é a distância de separação entre símbolos adjacentes e σ_N é o desvio padrão do ruído do canal. Para os três casos, a BER é, aproximadamente:

$$BER \approx \frac{SER}{log_2 M} \tag{11}$$

É válido ressaltar que, na teoria de comunicações sem fio, a SER e a BER são comumente vistas em função da razão sinal-ruído (*signal-to-noise ratio*, SNR) dada por $E_b/\aleph$, em que E_b é a enegia do bit e $\aleph$ é a densidade espectral de potência do ruído. Porém, a forma como foi apresentada no texto é mais apropriada para lidar com diagramas de

constelação de sinais ópticos. Conseguimos relacionar ambas as representações de BER e SER pelas seguintes equações (Lathi; Ding, 2012):

$$\sigma_N = \sqrt{\frac{\aleph}{2}} \tag{12}$$

$$E = E_b \cdot log_2 M \tag{13}$$

em que E é a energia média. Pela Fig. 6, podemos calcular a potência média da constelação QPSK a partir das distâncias dos pontos em relação à origem. Isso é feito somando o quadrado das distâncias de todos os pontos e dividindo pelo número de pontos (Lathi; Ding, 2012). A potência média relacionada com a distância adjacente entre símbolos para BPSK, QPSK e 16-QAM, respectivamente, é:

$$P_{BPSK} = \frac{d^2}{4} \tag{14}$$

$$P_{QPSK} = \frac{d^2}{2} \tag{15}$$

$$P_{16-QAM} = 2.5 \cdot d^2 \tag{16}$$

Para finalizar, observa-se que todos os processos a que o sinal é submetido contam com arquivos que permitem fazer as análises gráficas, conforme indicado pela Fig. 5. Todos os módulos geram gráficos no domínio do tempo, espectros, diagramas de constelação e histogramas de amplitudes do sinal para ajudar no processo de interpretação dos resultados.

Antes de começarmos a trabalhar com o *software* e começar a gerar resultados sobre a técnica, foi necessário analisar se os resultados obtidos pelo *software* desenvolvido eram compatíveis com aqueles previstos teoricamente. Por exemplo, a constelação gerada por um sinal QPSK corresponde a quatro pontos equidistantes da origem no plano I-Q, conforme a Fig. 6. Após um processo eficiente de encriptação, a constelação deve ter pontos aleatoriamente distribuídos por uma região circular e a BER do sinal encriptado dever ser maior que o limite de conseguir uma recepção livres de erros quando uma FEC é aplicada (Abbade *et al.*,). Esse limite da FEC foi considerado como $2 \cdot 10^{-3}$, que é o limite da segunda geração padronizada pela recomendação G.975.1 (2004) do ITU-T (TychopouloS; Koufopaulou; Tomkos, 2006). Vale ressaltar que existem FEC capazes de corrigir limites maiores que $2 \cdot 10^{-3}$, mas o uso de esquemas mais complexos, com maior sobrecarga e com recursos de correção mais fortes é vantajoso apenas para distâncias maiores (redes

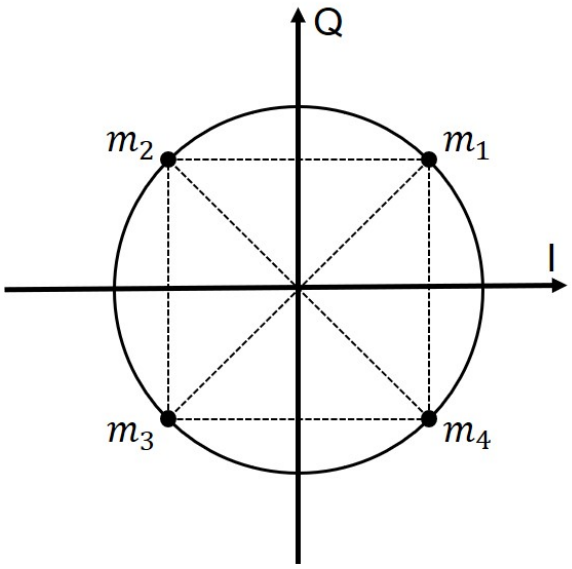

Figura 6 – Constelação para modulação QPSK previsto teoricamente.

submarinas, por exemplo). Além do mais, o uso de FECs mais complexas pode facilitar a recuperação do sinal criptografado. Já no processo de remoção da encriptação, os pontos devem retornar às quatro posições iniciais bem localizadas referentes à constelação do sinal QPSK (Fig. 6) e a BER deve tornar-se suficientemente pequena, talvez, menor que 10^{-15}, valor que consideramos livre de erros nas condições de simulações descrita a seguir: $R_s = 10$ GBaud, número de símbolos= 16384, $r = 0.1$, n_s= 902.

Na Fig. 7 temos os diagramas de constelação obtidos pelo KryptoSJ para o caso do sinal BPSK em banda-base. De fato, pelas Figs. 7 a) e c) podemos ver que as constelação de entrada e saída conferem com a teoria de um sinal que após modulado gera um sinal BPSK: dois pontos equidistantes da origem no plano I-Q, indicando que o sinal foi gerado e recuperado da maneira esperada. Além disso, a BER do sinal recuperado foi nula para ambos os métodos de cálculo discutidos anteriormente, isso confirma a boa recuperação do sinal. A Fig. 7 b) revela uma constelação com pontos aleatoriamente distribuídos por uma região circular, em distribuição gaussiana bidimensional e com uma BER igual a $0,5$, sugerindo o sucesso da técnica de encriptação utilizada.

As mesmas análises e conclusões podem ser tiradas para os sinais QPSK em banda-base (Fig. 8) e 16-QAM em banda-base (Fig. 9). Em QPSK em banda-base geramos e recuperamos os quatro pontos equidistantes da origem no plano I-Q em 8 a) e c) com BER zero. Em 16-QAM em banda-base, a BER igual a zero para o sinal recuperado também é

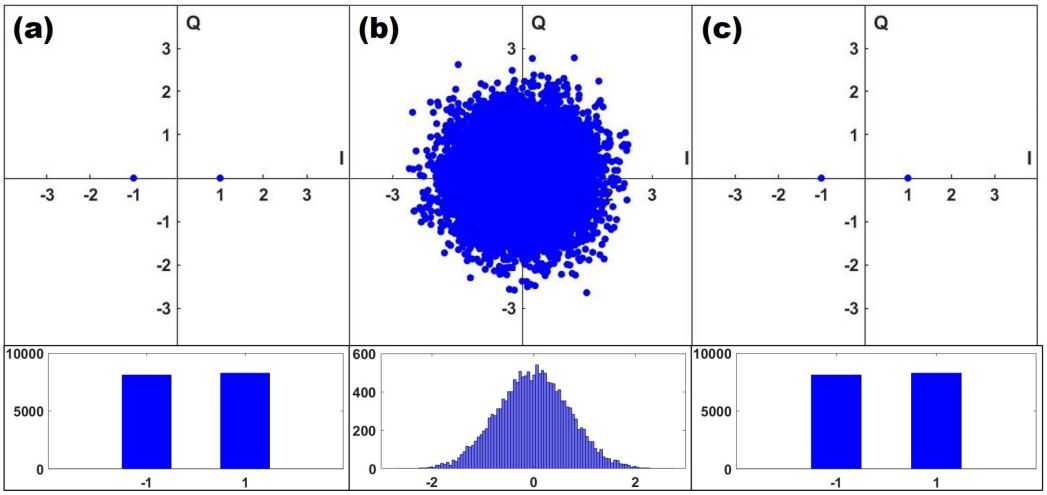

Figura 7 – Diagrama de constelação e histograma para o sinal BPSK em banda-base a) antes da criptografia, b) depois da criptografia DSP-SPE-Scr e, c) depois da remoção da criptografia.

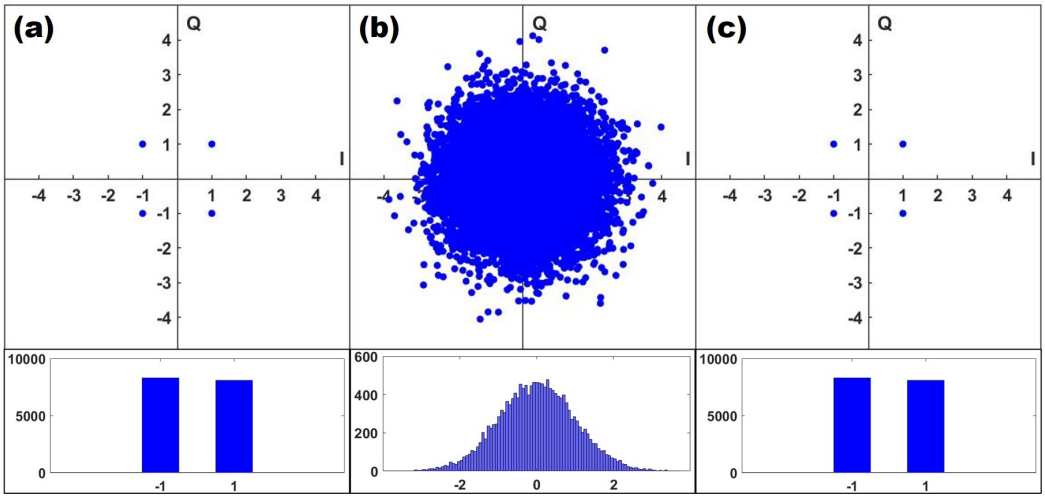

Figura 8 – Diagrama de constelação e histograma para o sinal QPSK em banda-base a) antes da criptografia, b) depois da criptografia DSP-SPE-Scr e, c) depois da remoção da criptografia.

alcançada, e os dezesseis pontos equidistantes também aparecem em 9 a) e c). As BERs para os sinais criptografados em ambos os casos também foram de $0,5$.

Uma outra maneira de conferir se o processo de criptografia está sendo feito de maneira coerente parte do fato de que a criptografia não introduz nenhuma perda na potência do sinal, pois apenas fases são alteradas. Portanto, a constelação de um sinal criptografado deve ter a mesma potência da constelação do sinal sem criptografia.

Como a constelação do sinal criptografado segue uma distribuição gaussiana bidimensional, sua potência é σ^2, a variância dessa gaussiana. Essa variância é a soma das

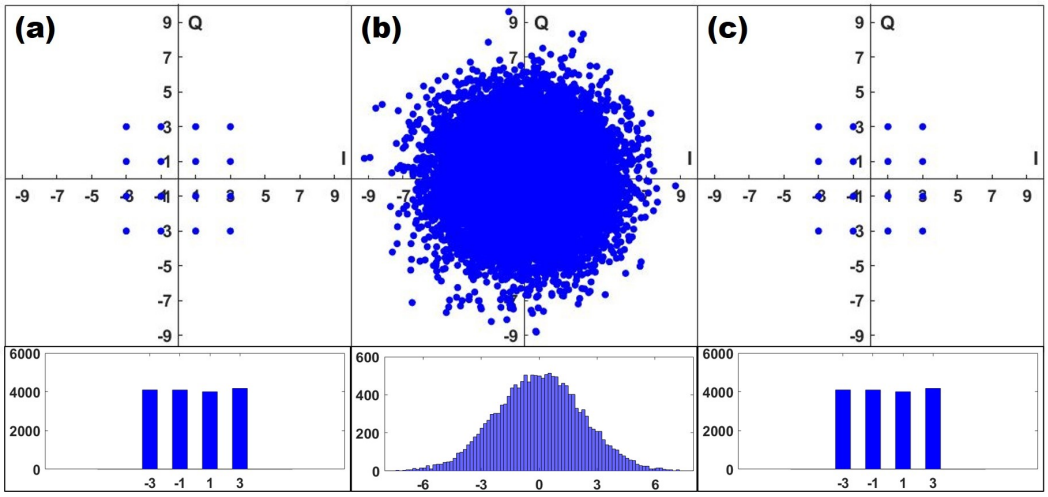

Figura 9 – Diagrama de constelação e histograma para o sinal 16-QAM em banda-base a) antes da criptografia, b) depois da criptografia DSP-SPE-Scr e, c) depois da remoção da criptografia.

variâncias associadas aos eixos I e Q, respectivamente, σ_x^2 e σ_y^2. Devido à simetria do problema, $\sigma_x^2 = \sigma_y^2$ e $\sigma^2 = 2\sigma_x^2$. A potência σ^2, deve ser igual às potências de cada constelação não criptografada, indicadas em (14)-(16). Em uma aproximação bastante razoável pode-se considerar que os pontos de uma gaussiana se concentram em um intervalo de $\pm$ 3 vezes seu desvio padrão. Considerando essa aproximação, é possível descobrir se as potências do sistema estão sendo mantidas e se o processo de criptografia é coerente. Os valores de 3σ encontrados foram: $3\sigma = 2.121$ para BPSK, $3\sigma = 3$ para QPSK e $3\sigma = 6.71$ para 16-QAM, que são aproximadamente os mesmo intervalos em que os pontos das gaussianas nas constelações das Figs. 7(b), 8(b) e 9(b) estão distribuídos.

Os resultados anteriores sugerem que o *software* KryptoSJ está atuando em conformidade com os resultados teóricos esperados. O próximo capítulo traz os resultados que foram obtidos para a transmissão de sinais criptografados a partir da nova técnica DSP-SPE-Scr.

4 Cenário de Simulação e Resultados

Como visto no capítulo anterior, o *software* responsável por tratar dos sinais em banda-base foi desenvolvido no Matlab® e chama-se KryptoSJ. Para as análises do sinal já modulado em uma portadora óptica e, posteriormente, propagado por enlaces de fibra óptica, as simulações são por encargo do *software* VPITransmissionMaker. Para isso, os resultados do *software* desenvolvido no Capítulo 3 serão utilizados como entrada para o VPITransmissionMaker. O resultado oferecido pelo VPITransmissionMaker será passado como entrada ao KryptoSJ que, então, removerá a encriptação de dados. A troca de dados entre o VPITransmissionMaker e o KryptoSJ poderá ser feita por meio da funcionalidade de co-simulação existente no VPITransmissionMaker. O esquema de troca de dados entre os *softwares* está ilustrado na Fig. 10.

A próxima seção tem como objetivo apresentar e descrever o cenário de simulação de um sistema coerente elaborado no VPITransmissionMaker para obter os resultados que serão mostrados nesse capítulo. Os parâmetros que foram utilizados no KryptoSJ continuam os mesmos já citados no Capítulo 3, exceto a taxa de símbolos, que foi ajustada para $R_s = 28$ GBaud. Assim, após a modulação óptica, teremos sistemas BPSK de 28 Gbps, um QPSK de 56 Gbps e um 16-QAM de 112 Gbps. Essa mudança se deve ao fato de que achamos interessante passar a levar em consideração os padrões comerciais vigentes, para possíveis aplicações comerciais. No VPITransmissionMaker trabalhamos com duas condições de simulações, que serão apresentadas em duas subseções: i) situação *back-to-back* (B2B) e, ii) situação com propagação.

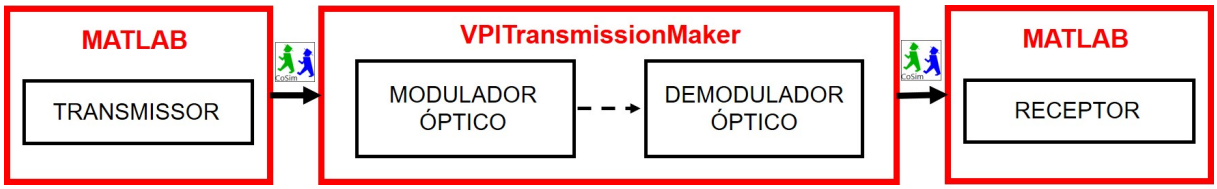

Figura 10 – Diagrama do funcionamento da co-simulação entre os *softwares*.

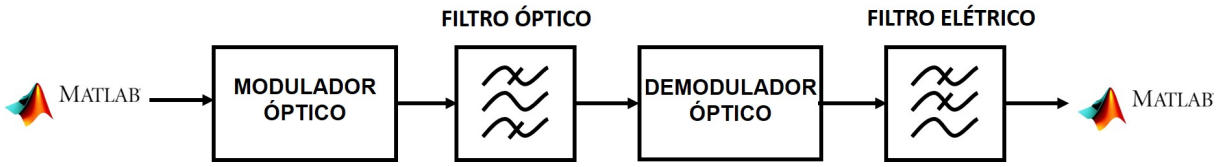

Figura 11 – Diagrama do cenário de simulação do VPITransmissionMaker em situação B2B.

4.1 Cenário de simulação

4.1.1 Situação *back-to-back*

Essa situação foi necessária para fazer as análises dos efeitos sofridos pelos sinais criptografados após a conversão para o domínio óptico. Como a maior diferença entre um sinal criptografado com processamento óptico de sinal e um sinal criptografado pela DSP-SPE-Scr é o fato do primeiro não necessitar passar por um processo de modulação óptica, é necessário analisar qual a penalidade que os processos de modulação e demodulação podem adicionar ao sinal recuperado.

Para essa análise, o cenário de simulação está ilustrado na Fig. 11. O módulo responsável por fazer a modulação óptica simula um modulador *Mach-Zehnder* e tem uma razão de extinção igual a 40 dB. Já o demodulador óptico simula um fotodetector com fotodiodos PIN com responsividade igual a 1 A/W e ruído térmico de $10 \cdot 10^{-12}$ A/$\sqrt{Hz}$. Os filtros óptico e elétrico têm como função diminuir a ação do ruído que pode ter sido adicionado no processo.

4.1.2 Situação com propagação

Essa situação de simulação nos permite verificar, a penalidade em distância experimentada por sinais criptografados com a DSP-SPE-Scr em relação a sinais que não estejam criptografados. Assim podemos estimar a penalidade de potência imposta pela DSP-SPE-Scr durante a propagação de sinais.

O processo de modulação óptica nessa situação é o mesmo da Fig. 11. Portanto, as configurações do módulo de modulação e demodulação são as mesmas já apresentadas anteriormente na Seção 4.1.1. Porém, para essa situação, foram adicionados diversos enlaces de 80 km cada de fibra monomodo padrão (*standard single mode fiber*, SSMF) entre o

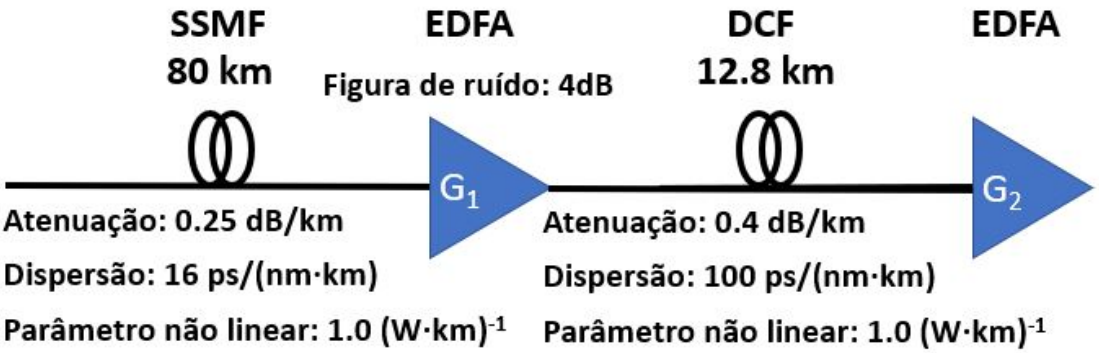

Figura 12 – Representação de um link óptico de simulação.

modulador e o filtro óptico da Fig. 11 no *software* VPITransmissionMaker. Para fazer a compensação da atenuação e da dispersão cromática imposta pela fibra, cada enlace é seguido de um amplificador de fibra dopada com érbio (*erbium-doped fiber amplifier*, EDFA) e de uma fibra compensadora de dispersão (*dispersion-compesating fiber*, DCF). A Fig. 12 ilustra como é a composição de cada link óptico, e traz as informações dos parâmetros utilizados na simulação. O amplificador G1 compensa a atenuação da SSMF enquanto G2 compensa a atenuação causada pela DCF. O ganho de G1 e G2 são dados pela equação:

$$G_{dB} = \alpha \cdot L \tag{17}$$

em que G_{dB} é o ganho dado em decibéis, α é a atenuação e L o comprimento da fibra a ser compensada.

A próxima seção descreve todas as atividades que foram desenvolvidas para interpretação e análise dos resultados.

4.2 Resultados e Discussões

Essa seção traz todos os resultados necessários para uma avaliação profunda acerca da DSP-SPE-Scr. Além disso, aqui encontram-se as discussões levantadas em cada resultado. Para facilitar a leitura, os resultados foram separados em subseções. A seguir, a primeira seção traz a análise da segurança da técnica contra BFA.

4.2.1 Análise da segurança da técnica DSP-SPE-Scr

Qualquer técnica de criptografia está sujeita a ataques que permitam a identificação da chave criptográfica utilizada. Nessa seção, é nosso objetivo identificar um desses ataques, os chamados ataques de força bruta. Um BFA consiste em um teste de tentativa e erro. Um invasor verifica quais são todas as chaves possíveis para aquele sistema e utiliza cada possibilidade, uma por vez, em busca de uma mensagem que faça sentido.

Para analisar a segurança da técnica DSP-SPE-Scr a esse tipo de ataque, precisamos separar a técnica em duas etapas. Primeiro vamos levar em consideração apenas a operação da técnica SPE. Nessa situação, precisamos considerar que é possível recuperar o sinal mesmo com um certo erro, ou diferença média, de $\pm\Delta\theta$ em cada uma das n_s fatias espectrais. Portanto, se a fase da i-ésima fatia é θ_i e o intruso adotar uma fase $\theta_{intruso,i} = \theta_i \pm \Delta\theta$, o sinal original ainda pode ser recuperado até o limite da FEC. O KryptoSJ foi adaptado para permitir a análise dessa situação. Considerando essa abordagem, o número possível de fases por fatias que um intruso precisa avaliar é de $\frac{360}{2\Delta\theta}$. Como nossa chave criptográfica é composta de n_s fatias, seriam necessárias $\left(\frac{360}{2\Delta\theta}\right)^{n_s}$ tentativas para que um ataque seja bem sucedido.

A análise dos resultados da primeira parte dessa atividade nos diz qual é o máximo erro, $\pm\Delta\theta_{max}$, que o usuário não autorizado pode ter em cada fatia para conseguir recuperar os dados do sinal. Esse erro foi considerado como uma variável aleatória uniformemente distribuída de $-\frac{\Delta\theta}{2}$ à $+\frac{\Delta\theta}{2}$. Para conseguir esse valor de $\Delta\theta_{max}$, foi necessário realizar simulações para vários valores de $\Delta\theta$, até a BER atingir o valor máximo que pode ser recuperada pela FEC, que é $2 \cdot 10^{-3}$.

É importante ressaltar que, para essa análise de resultados, nenhuma modulação óptica foi considerada, ou seja, nos limitamos a trabalhar apenas no *software* KryptoSJ.

A Figura 13 mostra um gráfico da BER em função de $\Delta\theta$ para os três tipos de sinalização. Para os resultados desse gráfico, o *software* foi colocado em um *loop* para rodar 50 vezes e, em seguida, retornar com a BER média. As operações a respeito da técnica de embaralhamento intracanal estavam desligadas. Os valores de $\Delta\theta_{max}$ encontrados para cada tipo de sinalização são apresentados na Tabela 1.

Para entender esses resultados, é interessante fazer uma comparação com o AES-256, um padrão de criptografia de dados usado até mesmo para aplicações ultrassecretas

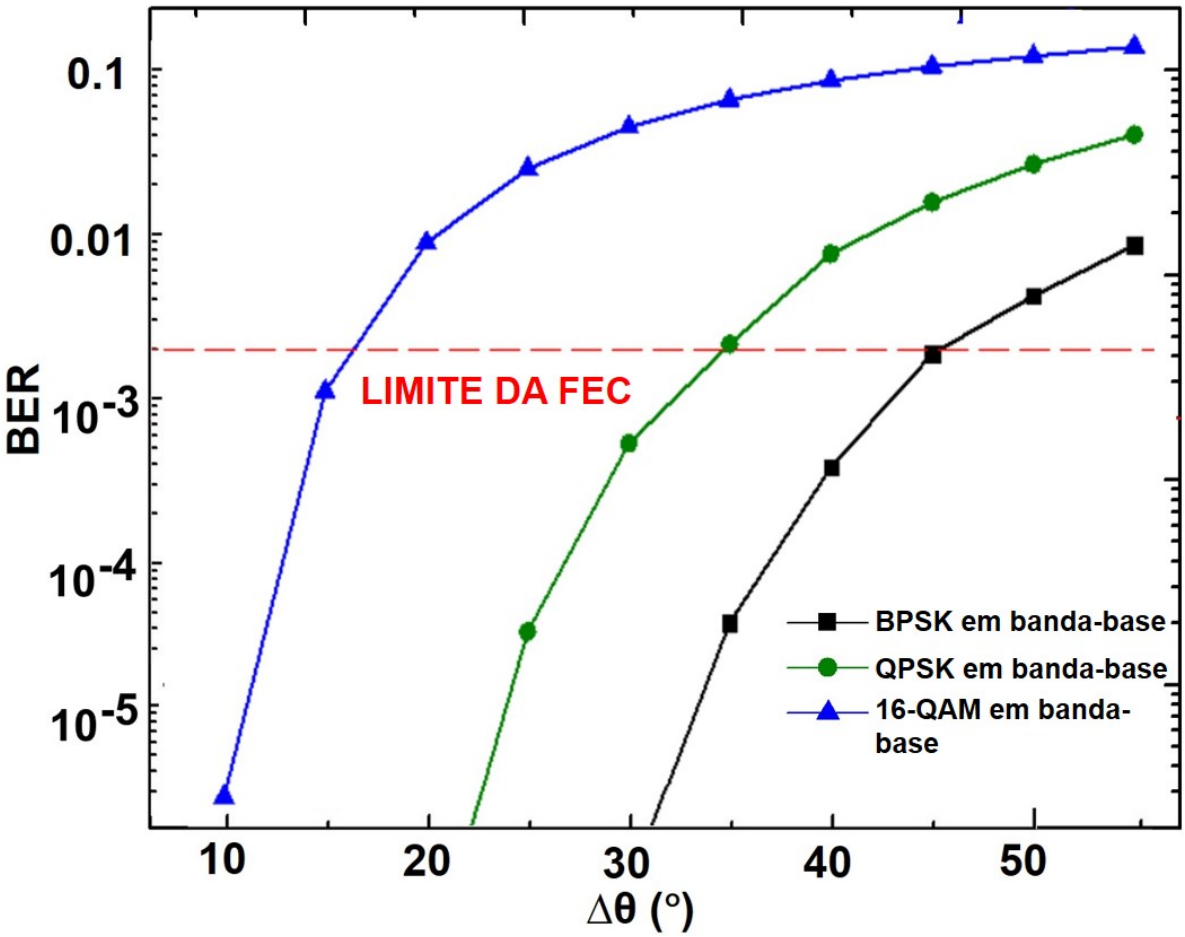

Figura 13 – Gráfico da BER em função de $\Delta\theta$ para as três diferentes sinalizações.

Tabela 1 – Segurança da DSP-SPE-Scr

Modulação	$\Delta\theta_{máx}$	n_s	n_t (SPE)	n_t (e.i.**)	n_t total
BPSK em b-b*	46°	94	10^{83}	$94! = 10^{146}$	$10^{83+146} = 10^{229}$
QPSK em b-b*	33°	78	10^{80}	$78! = 10^{115}$	$10^{80+115} = 10^{195}$
16-QAM em b-b*	15°	60	10^{82}	$60! = 10^{81}$	$10^{82+81} = 10^{163}$

*banda-base, **embaralhamento intracanal

internacionais. O número de tentativas n_t que o AES-256 requer que o intruso realize para que um BFA seja bem sucedido é $n_t = 2^{256} = 10^{77}$. Comparando esse número com os resultados da Tabela 1, podemos concluir que a DSP-SPE sozinha já é uma técnica robusta que pode oferecer segurança maior ou igual à do AES-256 para um número relativamente baixo de fatias. De fato, as simulações anteriores utilizaram mais de 900 fatias, número bem maior do que o valor de 94 necessárias para o BPSK em banda-base, que é a modulação que necessita de um número maior de fatias. No caso, a criptografia do BPSK em banda-base é a mais fácil de ser "quebrada", porque tem um número menor de símbolos e por isso uma chave mais curta. Por esse motivo, para aumentar a chave e igualar a segurança com

as outras sinalizações, o BPSK em banda-base necessita de um número de fatias maior. A mesma explicação se repete ao perceber que o QPSK em banda-base precisa de mais fatias que o 16-QAM em banda-base.

Para ilustrar graficamente a influência de erros na identificação de sinais em BFA, a Figura 14 traz os histogramas para diferentes $\Delta\theta$ no caso BPSK em banda-base. Podemos observar que a distribuição está concentrada nas amplitudes -1 e 1 para o sinal criptografado. Na medida que $\Delta\theta$ aumenta, a distribuição começa a se tornar gaussiana ao redor de -1 e 1. Se o aumento for suficientemente elevado, as gaussianas começam a se sobrepor até que se tornem indistinguíveis. É importante notar que as figuras são válidas para os casos em que $\Delta\theta$ é igual para todas as fatias. Se apenas uma ou poucas fatias tiverem $\Delta\theta$ dentro dos limites indicados, a distribuição continuará Gaussiana.

De fato, apesar de apenas considerando as operações da SPE já ter sido constatado que a técnica é segura contra BFA, ainda podemos incluir a análise das operações do embaralhamento intracanal. O número de permutações possíveis é $n_s!$. Considerando os mesmos números de fatias encontrados para a SPE, os números de tentativas para quebrar as operações do embaralhamento intracanal estão dispostos na Tabela 1. Uma vez que temos n_t para um BFA ser bem-sucedido tanto para a técnica SPE quanto para a de embaralhamento intracanal, podemos mensurar qual a robustez da nova técnica DSP-SPE-Scr. Para isso, basta multiplicar os valores de n_t da SPE e da operação de embaralhamento intracanal dispostos nas Tabelas 1: $n_t = 10^{229}$ para BPSK em banda-base, $n_t = 10^{195}$ para QPSK em banda-base e $n_t = 10^{163}$ para 16-QAM em banda-base.

4.2.2 Análise dos efeitos sofridos pelos sinais criptografados em banda-base

Uma vez que sabemos que adicionar operações de embaralhamento intracanal na técnica DSP-SPE faz com que a robustez contra BFA aumente significativamente, precisamos analisar se essas operações também trazem alguma penalidade no desempenho do sinal. Para isso, mais uma funcionalidade foi acrescentada ao *software* descrito no Capítulo 3. Essa funcionalidade consistiu na simulação de um canal com AWGN. Alguns valores de desvio de padrão de ruído σ_n foram fixados na rotina, enquanto o programa estava em um *loop* para rodar cem vezes. Cada vez que o programa rodava, gerava um sinal de entrada diferente, primeiro BPSK em banda-base criptografado pela DSP-SPE,

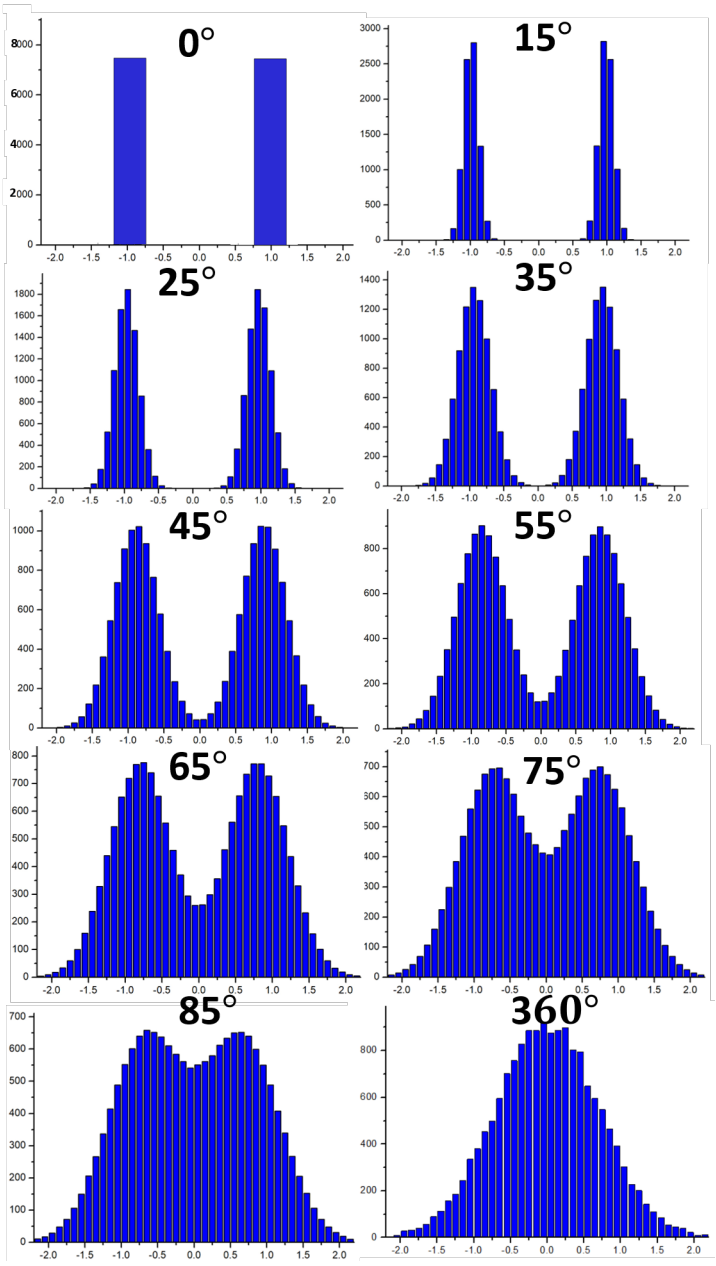

Figura 14 – Histogramas para o caso BPSK em banda-base para diferentes valores de flutuação de fase ($\Delta\theta$) ao redor da fase de encriptação.

depois criptografado pela DSP-SPE-Scr e depois sem criptografia. Isso foi repetido também para os sinais QPSK e 16-QAM em banda-base. Depois foi feita a média dos cem valores de BER obtidos para cada desvio padrão e essas médias de BER obtidas para cada ponto foram graficadas em um gráfico de BER *vs.* SNR, conforme a Fig. 15.

As curvas da Fig. 15 nos mostra um resultado muito importante. Além de observamos que adicionar as operações de embaralhamento intracanal ao DSP-SPE não causa penalidade para o desempenho dos sinais, ainda fazemos a mesma observação para um sinal sem criptografia. Ou seja, um sinal criptografado pela DSP-SPE-Scr não difere de

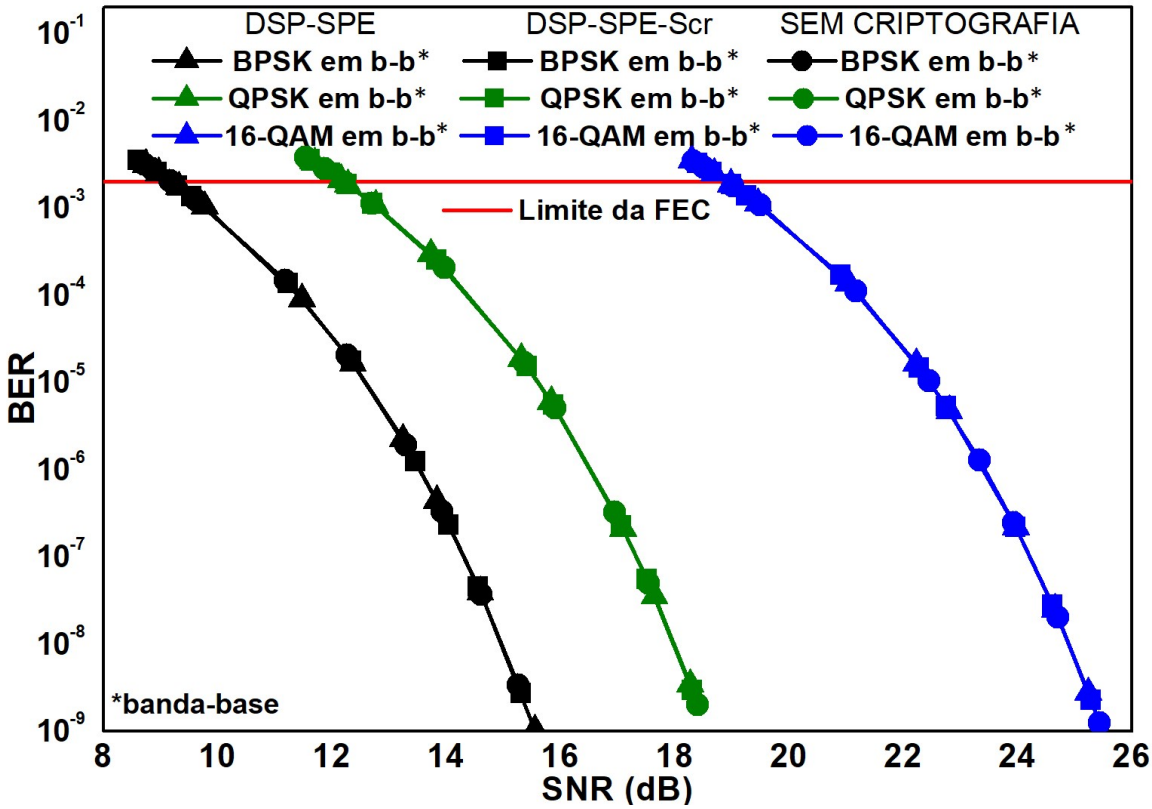

Figura 15 – Gráfico dos valores médios de BER em função da SNR para diferentes sinais e técnicas de criptografia aplicados a sinais em banda-base.

um sinal que não passa por nenhum processo de criptografia em relação a desempenho no domínio digital. Para o próximo passo, precisamos analisar as penalidades que são introduzidas pela DSP-SPE-Scr no desempenho do sinal após a modulação óptica.

4.2.3 Análise dos efeitos da conversão para o domínio óptico

Essa análise foi realizada em situação B2B, utilizando o cenário de simulação descrito na Subseção 4.1.1. Os resultados dessa subseção estão divididos em duas etapas:

1. Foi verificado se as BERs dos sinais encriptados e desencriptados são próximas àquelas mencionadas no Capítulo 3. Em princípio, espera-se que os processos de conversão eletro-óptica e óptico-elétrica degradem, mas não em demasia, essas BERs;
2. Foi comparada a BER do sinal encriptado e desencriptado com aquela de um sinal que não tenha sido encriptado. Essa comparação foi feita em função da razão sinal-ruído óptica (*optical signal-to-noise ratio*, OSNR). Esse procedimento foi capaz de avaliar a penalidade introduzida pela DSP-SPDE.

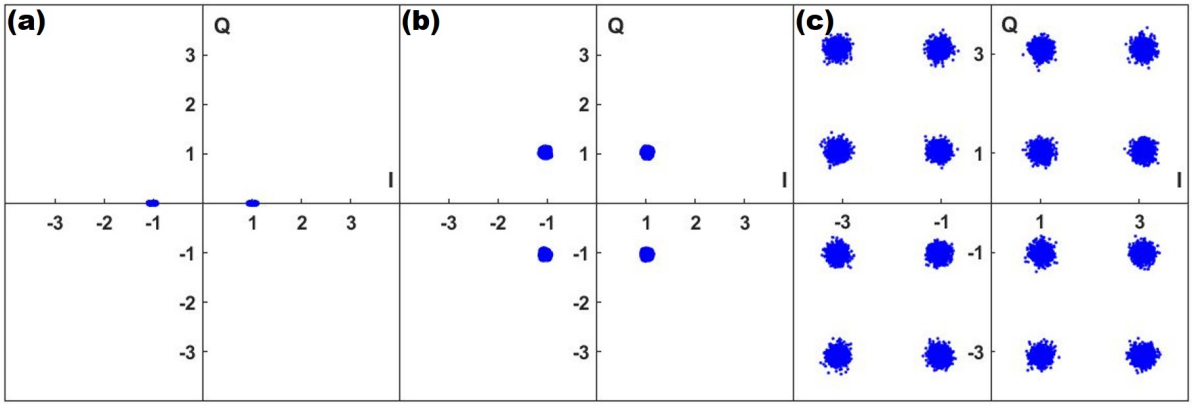

Figura 16 – Diagrama de constelação dos sinais após a remoção da criptografia para os sinais com modulações ópticas a) BPSK, b) QPSK e, c) 16-QAM.

Começando pela primeira etapa, como já dito, esperava-se que os processos de conversão eletro-óptica e óptico-elétrica, considerados degradassem apenas marginalmente o sinal. De fato, as simulações comprovaram que, em situação B2B, as conversões óptico-elétrica e eletro-óptica sobre sinais banda-base criptografados, independentemente de sua modulação (BPSK, QPSK ou 16-QAM), não causam impactos significativos na taxa de erro de bit. Em todos os casos, a BER foi inferior a 10^{-15}, assim os sinais desencriptados podem ser considerados livres de erros, como explicado no Capítulo 3.

Essa verificação também pode ser feita a partir da Fig. 16. Ela mostra os diagramas de constelação do sinal recuperado para as diferentes modulações. Percebemos que, assim como as Figs. 7c), 8c) e 9c), os pontos são muito bem definidos, apenas apresentam um leve ruído que não afeta significativamente a recepção. Esse pequeno ruído que aparece nos diagramas de constelação e sua possível causa será melhor discutido na próxima análise dessa subseção.

Após a constatação de que as conversões eletro-óptica e óptico-elétrica, necessárias na nova técnica DSP-SPE-Scr, degradaram apenas marginalmente o sinal a ser propagado, nossa próxima análise compara, em função da OSNR, a BER do sinal encriptado e desencriptado com a BER de um sinal que não tenha sido encriptado. Isso nos permitiu saber se a nova técnica de criptografia insere uma penalidade muito grande no sinal.

Para essa análise, foi necessário incluir entre o modulador e o demodulador óptico da Fig. 10, uma fonte AWGN. Vale relembrar que o número de símbolos simulados em todos os casos é 16384, portanto, temos 16384 bits simulados no caso BPSK, 32768 bits para QPSK e 65536 para 16-QAM. A densidade espectral de potência do AWGN foi

variada de forma a atingir um valor de BER menor que o limite da FEC. Essa análise foi feita para os três tipos de modulações e está apresentada na Fig. 17.

Pelas curvas referentes ao caso 16-QAM, podemos perceber que a DSP-SPE-Scr insere uma certa penalidade em valores de BER muito baixos. Isso provavelmente acontece porque a modulação óptica é um processo não linear, que pode atuar de maneira diferente em sinais com amplitudes maiores. O processo de criptografia faz com que a distribuição de potência do sinal criptografado seja diferente daquela relacionada a um sinal não-criptografado, conforme podemos verificar nos histogramas de amplitude da Fig. 18, que ilustra esse efeito para um sinal BPSK em banda-base. Nota-se que o sinal de entrada tem amplitudes bem concentradas em -1 e 1. Já as amplitudes do sinal criptografado obedecem uma distribuição aproximadamente gaussiana, cujas amplitudes se estendem por valores que estão além do intervalo -2 a 2.

Porém, conforme observamos na Fig. 17, quando a OSNR diminui, a penalidade do ruído passa a ser dominante na análise e a BER para o caso em que o sinal passou pelo processo da DSP-SPE-Scr é muito próxima àqueles casos em que o sinal não passou por nenhum processo de criptografia.

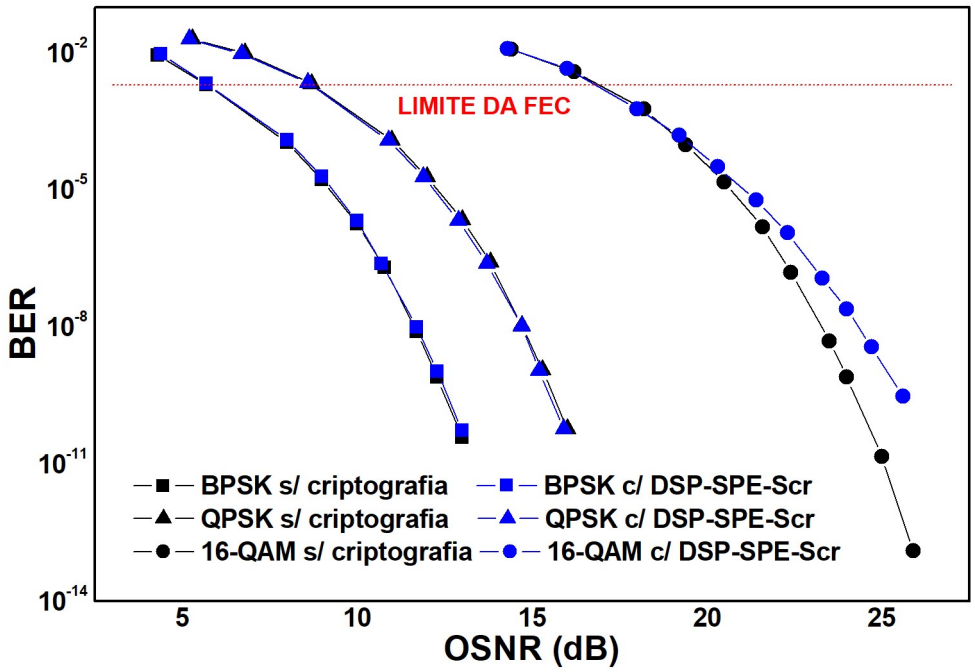

Figura 17 – Gráfico da BER em função da OSNR para análise da penalidade da técnica para os diferentes tipos de modulação.

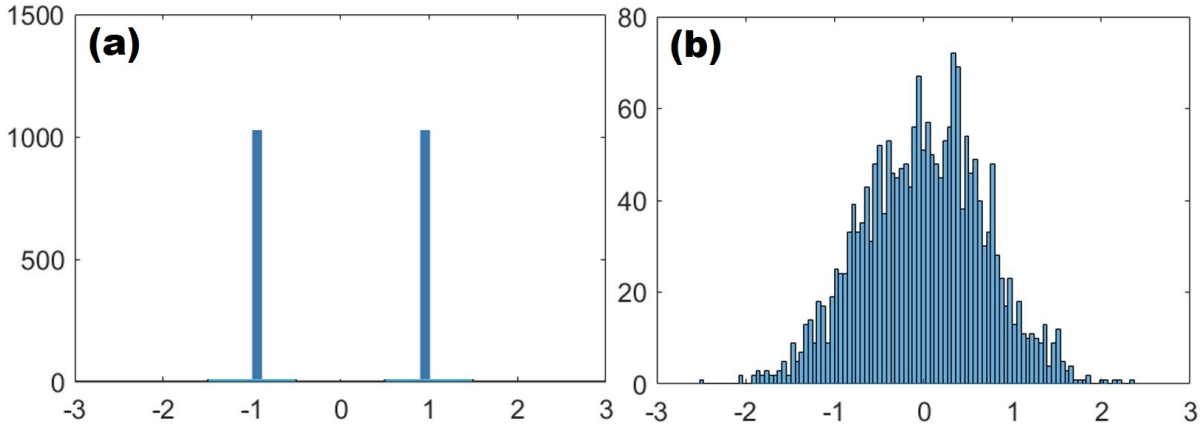

Figura 18 – Histograma de amplitudes para (a) o sinal de entrada e (b) o sinal após a criptografia DSP-SPE-Scr.

Para os casos BPSK e QPSK, quando a OSNR é tão alta quanto à do 16-QAM, também é possível perceber esse comportamento. Porém, nessas situações a BER é tão baixa que dificilmente poderia ser medida em sistemas práticos. Por essa razão, as curvas da Fig. 17 não ilustram esse comportamento.

Esse resultado mostra que a técnica DSP-SPE-Scr não insere penalidade significativa no desempenho da transmissão dos sinais, pois no limite da FEC, que é nosso ponto de maior interesse, as curvas de todas as modulações estão praticamente sobrepostas. Isso torna a DSP-SPE-Scr uma estratégia com potencial para aplicações práticas.

4.2.4 Análise da DSP-SPE-Scr após a propagação por enlaces ópticos

Utilizando agora o cenário de simulação da Seção 4.1.2, essa análise permitiu verificar, por meio de simulações numéricas, a penalidade em distância experimentada por sinais criptografados com a DSP-SPE-Scr em relação a sinais que não estejam criptografados.

Como visto na subseção anterior, por conta dos efeitos não-lineares, alguns dispositivos ópticos podem atuar de maneira diferente em sinais criptografados, devido a diferente distribuição de potência. Assim, como é sabido que a fibra óptica introduz não-linearidades, como a automodulação de fase (*self-phase modulation*, SPM), também se espera inicialmente que essa diferença de distribuição de potência possa interferir de forma negativa no alcance de propagação de sinais criptografados. Por isso, torna-se importante estimar o impacto dessa redução para sistemas práticos.

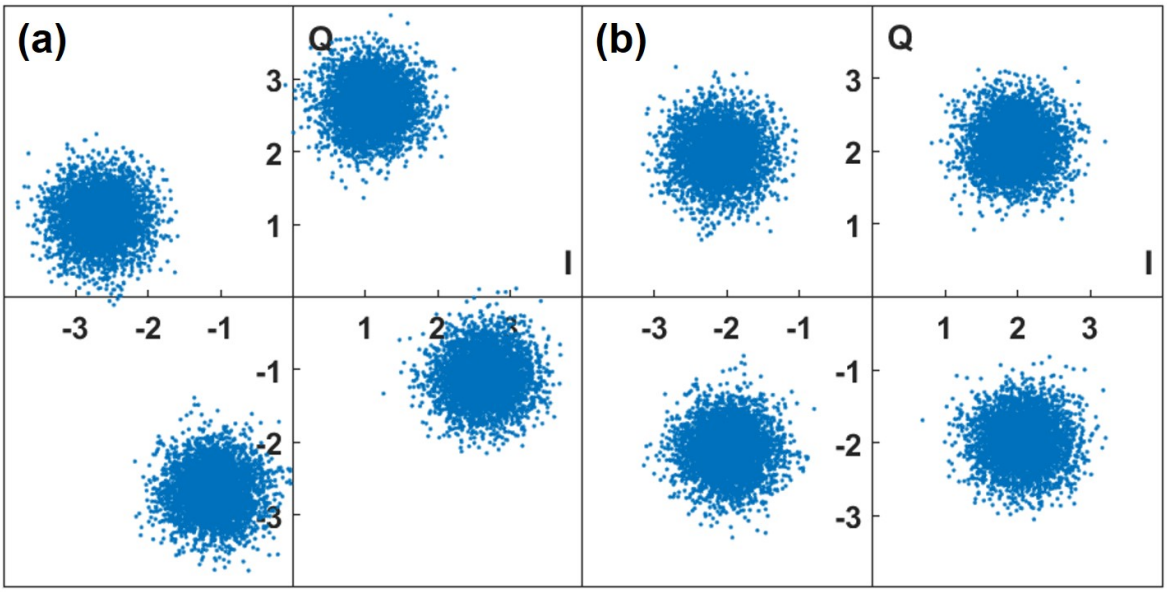

Figura 19 – Diagramas de constelação de uma modulação QPSK (a) antes e (b) depois do código de compensação de fase.

Iniciando a coleta de resultados, notou-se que, ao lidar com as não-linearidades da fibra, o modelo de simulação fica mais complexo e a dispersão acaba influenciando também na fase do sinal de maneira linear. Devemos relembrar que o alargamento temporal de pulsos devido à dispersão resulta da dependência da constante de propagação β em relação à frequência. Na condição $f - f_0 << f_0$, expandindo $\beta(f)$ em uma série de Taylor em torno da frequência central f_0, obteremos os coeficientes de $\beta(f)$ que podem ser retidos até a teceira ordem (Agrawal, 2014):

$$\beta(f) \approx \beta_0 + \beta_1(\Delta f) + \frac{\beta_2}{2}(\Delta f)^2 + \frac{\beta_3}{6}(\Delta f)^3 \tag{18}$$

em que $\Delta f = f - f_0$, $\beta_1 = \frac{1}{v_g}$ sendo v_g a velocidade de grupo, β_2 é o coeficiente da dispersão de velocidade de grupo (*group-velocity dispersion*, GVD) e β_3 é o parâmetro de dispersão de terceira ordem, que está relacionado com à inclinação da dispersão (*dispersion slope*, S). O coeficiente β_0 é o coeficiente linear que influencia na fase do sinal. Uma vez notado isso, foi necessário incluir na rotina do receptor do KryptoSJ um código para compensar esse desvio de fase. O funcionamento dessa compensação está ilustrado para uma modulação QPSK pela Fig. 19. Vale ressaltar que a compensação foi necessária para todas as modulações e distâncias de propagação apresentadas no trabalho.

Passando para os resultados, como esperado, os sinais não criptografados conseguem maior alcance considerando o limite da FEC. Pelo gráfico da Fig. 20 podemos perceber

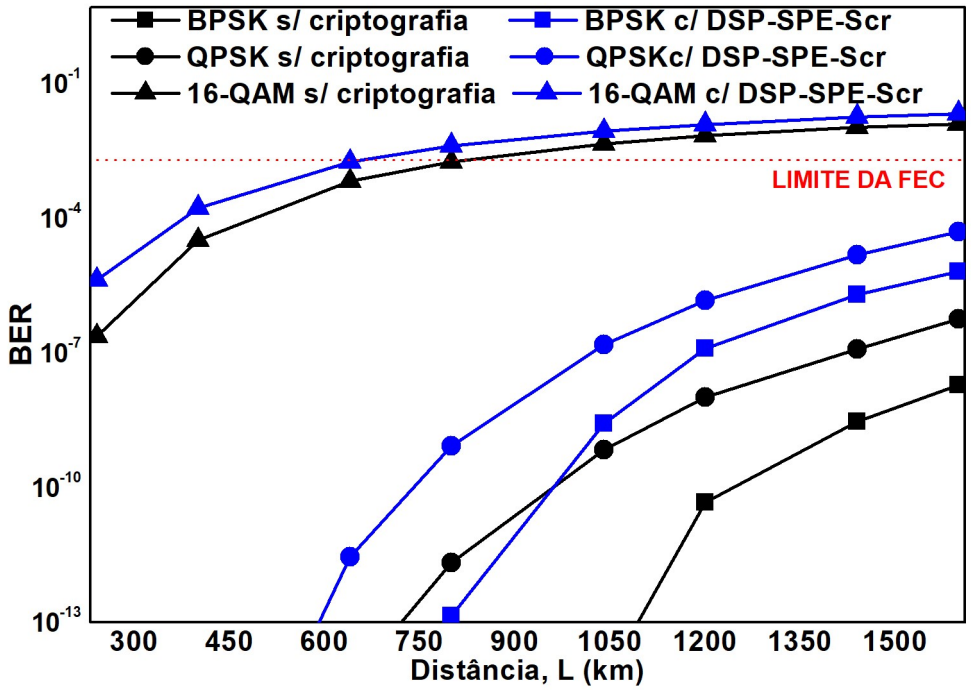

Figura 20 – Gráfico da BER em função do comprimento da fibra para análise do alcance de sinais criptografados em relação aos não criptografados.

que um sinal 16-QAM não criptografado consegue trafegar por aproximadamente 160 km a mais do que um sinal criptografado. Uma possível explicação para isso seria dada pelos efeitos não-lineares que são mais significativos em sinais com maiores amplitudes, conforme já comentado anteriormente. Nota-se também que, assim como no gráfico da Fig. 17, para ruídos de maior potência, a diferença da taxa de erro de bit vai diminuindo, porque os efeitos do ruído passam a ser predominantes. Os casos BPSK e QPSK conseguem alcances muito maiores que os de rede metropolitanas (foco desse trabalho) e, por isso, não são apresentados. Porém, vale ressaltar que a distância entre essas curvas também tende a diminuir para maiores valores de BER.

Por fim, apesar de conseguir um alcance menor, um sinal 16-QAM com DPS-SPE-Scr ainda pode trafegar por redes metropolitanas com diâmetro de 640 km e ser recuperado livre de erros pela FEC. Isso sugere que a DSP-SPE-Scr possa ser usada em sistemas comerciais.

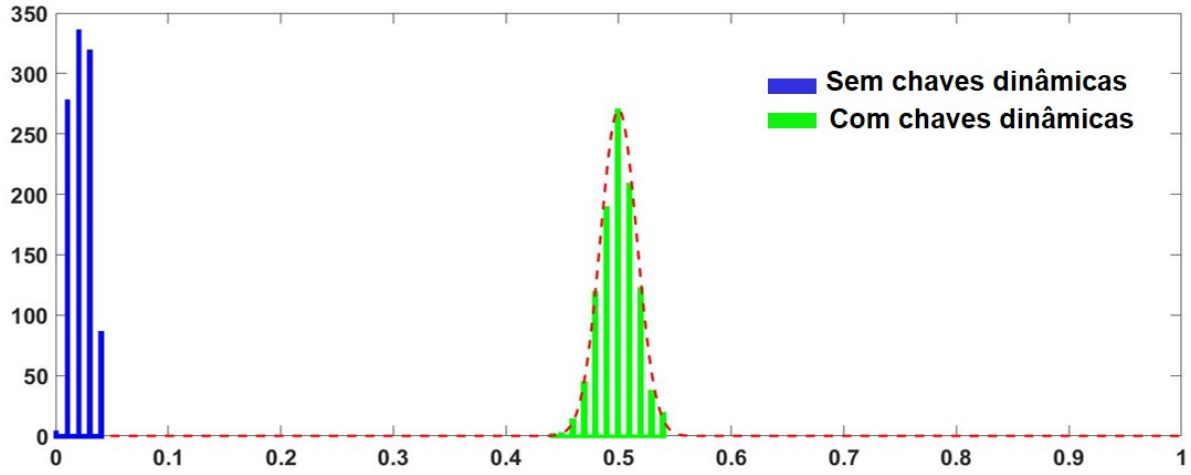

Figura 21 – Histograma para análise da propriedade de difusão com e sem chaves dinâmicas.

4.2.5 Análise da difusão, confusão e segurança semântica

Como dito na Seção 1.1, as propriedades de difusão e confusão de Shannon e a segurança semântica precisam ser satisfeitas para que uma cifra seja segura. Para conseguir testar essas propriedades, foi necessário adicionar uma funcionalidade ao KryptoSJ.

Para a difusão, um bit da mensagem de entrada, que continha 1024 bits totais, era alterado a cada rodada. O programa estava em um *loop* para rodar 1025 vezes, assim a primeira rodada era a de referência e as outras garantiam que todos os bits da mensagem de referência passassem por uma mudança. A cada rodada, os bits da nova mensagem criptografada eram comparados com os bits da rodada de referência, que deveriam mudar em aproximadamente 50% para garantir a propriedade de difusão. Antes de aplicar as chaves dinâmicas descritas na Seção 2.2, apenas 4% dos bits dos sinais criptografados eram diferentes, conforme a Fig. 21. Por esse motivo, fez-se necessário a utilização dessas chaves que variam dinamicamente entre um bloco e outro. Os códigos necessários para aplicar a chave dinâmica na técnica DSP-SPE e testar as propriedades de Shannon foram escritos pelo aluno Welerson Santos Souza, membro do nosso grupo de pesquisa, a partir de seu projeto de mestrado (Souza; Abbade, 2019). As adaptações para a técnica DSP-SPE-Scr foram feitas pela autora desse trabalho. Os resultados obtidos das porcentagens de bits alterados a cada rodada utilizando chaves dinâmicas pode ser conferido na Fig. 21.

Pelo histograma em verde, podemos perceber que os resultados proporcionaram uma gaussiana com centro em 50%. Isso indica que a propriedade de difusão é satisfeita ao utilizar chaves dinâmicas no sistema.

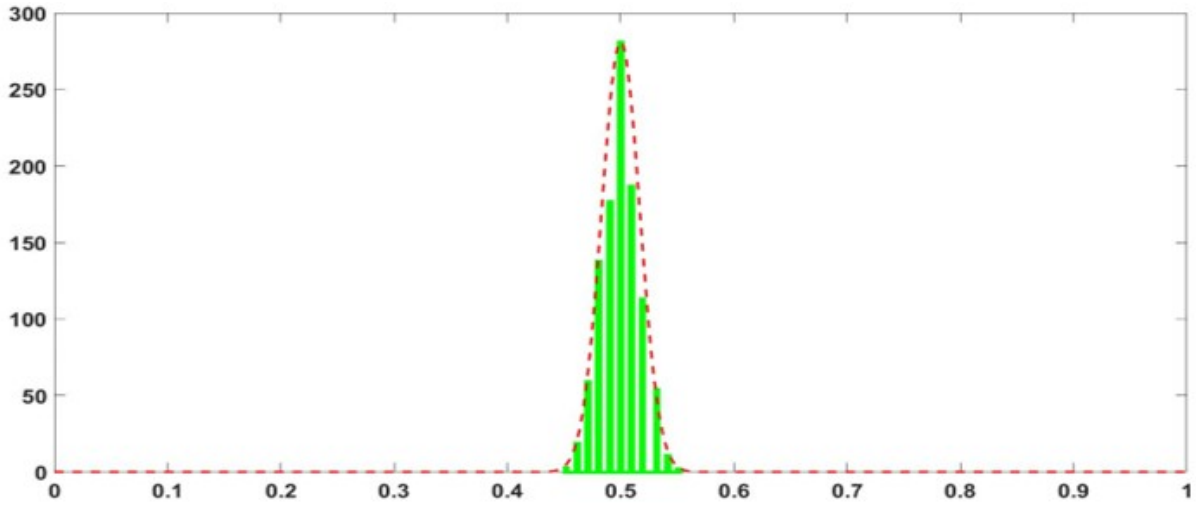

Figura 22 – Histograma para análise da propriedade de confusão com chaves dinâmicas.

Para a propriedade de confusão, seguimos o mesmo conceito de chaves dinâmicas e aplicamos a lógica da difusão. Porém, ao invés de alterarmos os bits da mensagem de entrada, alteramos os bits da chave inicial K_i. Como a chave possuía um tamanho total de 522 bits, foi necessário colocar o programa em um loop para rodar 523 vezes. Os bits da mensagem criptografada foram monitorados a cada rodada e comparados com a rodada de referência. Com os resultados obtidos utilizando chaves dinâmicas, foi plotado o histograma da Fig. 22, que nos traz a mesma conclusão obtida com o teste de difusão.

Já para avaliar a segurança semântica, utilizou-se a mesma sequência de bits em todas as rodadas. O programa foi executado em um laço de 1025 rodadas e todos os blocos de mensagem criptografada foram comparados entre si. Ao obter a matriz com essa comparação, de tamanho 1025x1025, levantou-se o histograma da Fig. 23. Mais uma vez, utilizando chaves dinâmicas, temos o resultado satisfatório de uma gaussiana com centro em 50%. Uma outra maneira de analisar o resultado de segurança semântica é a partir do mapa de cores tridimensional da Fig. 24. Como esperado, a quantidade de bits diferentes é simétrica em relação a diagonal do mapa, onde o mínimo valor zero é obtido. Fora dessa diagonal, a quantidade de bits diferentes é próxima de 50%, levando à segurança semântica.

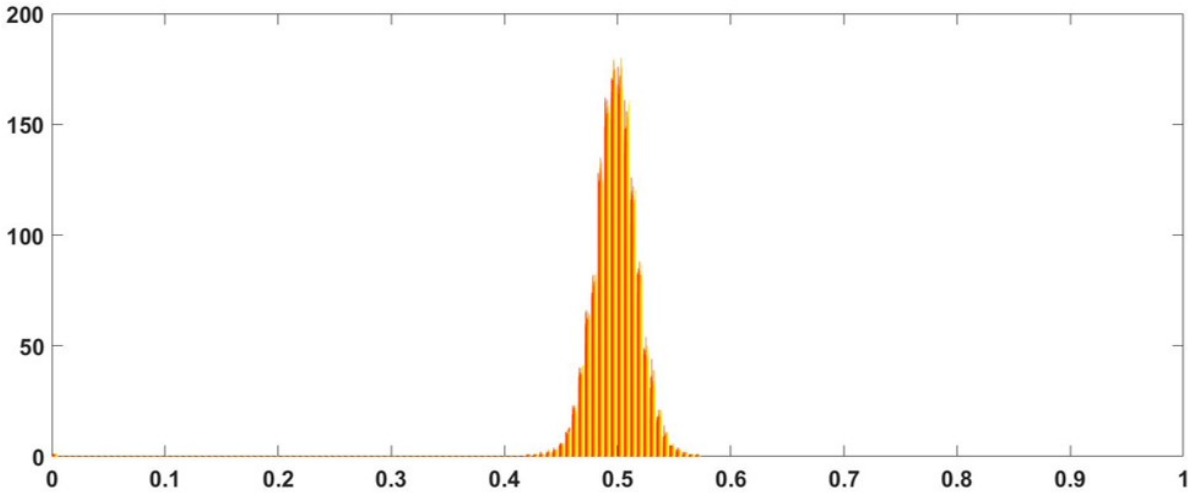

Figura 23 – Histograma para análise de segurança semântica com chaves dinâmicas.

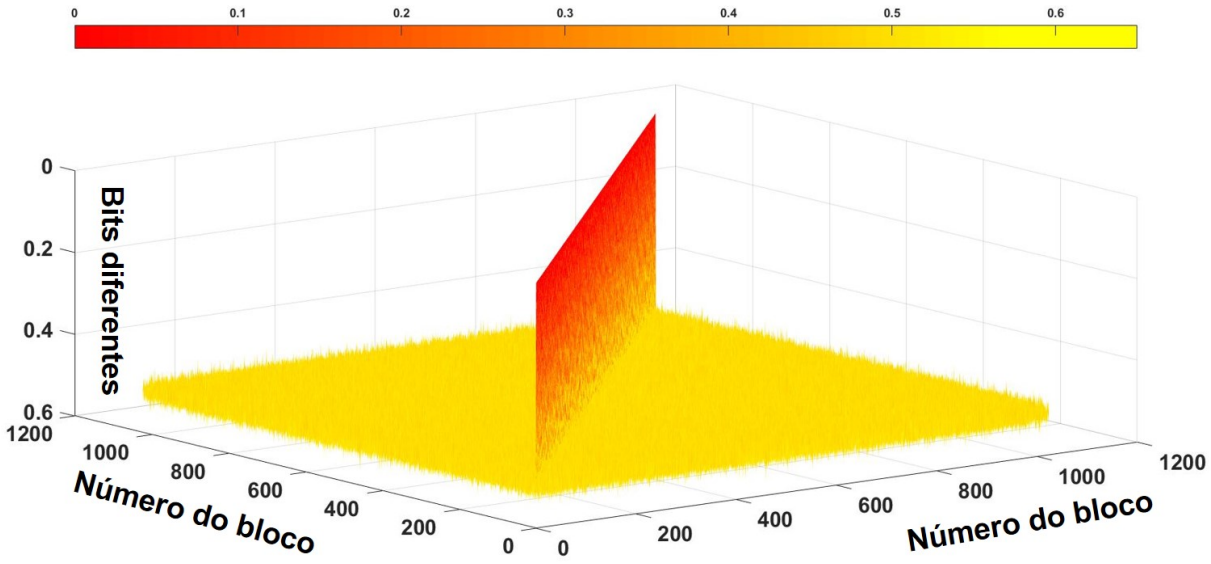

Figura 24 – Mapa de cores para análise de segurança semântica com chaves dinâmicas.

4.2.6 Avaliação experimental da DSP-SPE

O grupo de pesquisa no qual a autora desse trabalho está inserida fez uma parceria com a Fundação CPqD para a realização de um experimento físico acerca da implantação da DSP-SPE. Um teste inicial foi feito pelo pesquisador Sandro Marcelo Rossi, da fundação CPqD. Esse teste foi realizado usando os resultados do código desenvolvido no Capítulo 3 como entrada para um experimento físico montado na Fundação CPqD. O teste foi feito para um QPSK de 40 Gbps em polarização única.

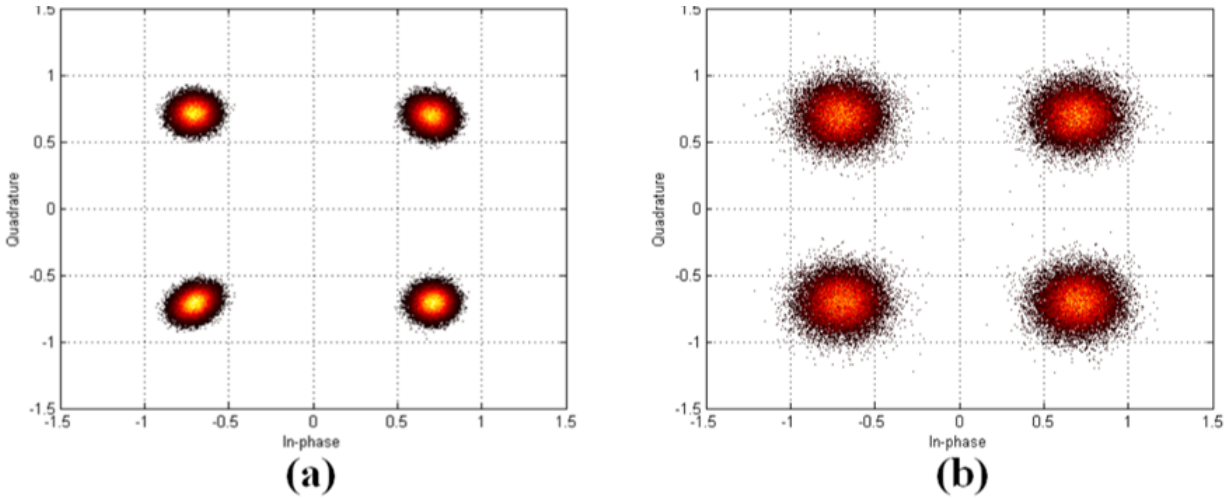

Figura 25 – Diagramas de constelação da (a) entrada e (b) saída de um teste inicial para um sinal QPSK criptografado em um experimento físico.

No domínio óptico, inicialmente, o sinal criptografado foi transmitido diretamente para o receptor, sem passar por nenhum enlace de fibra (B2B). O sinal então foi demodulado e processado pelas rotinas de remoção de criptografia do KryptoSJ. Todo esse processamento foi realizado *off-line*, ou seja, sem conexão direta entre transmissor e receptor. A Fig. 25 mostra os resultados para esse primeiro teste.

As Figs. 25(a) e (b) mostram, respectivamente, as constelações dos sinais criptografado e desencriptado. A última dessas constelações indica uma BER de $\approx 10^{-9}$, bem abaixo do limite da FEC, e revela o potencial de utilização prático da DSP-SPE. Como a DSP-SPE-Scr não introduz penalidades adicionais a DSP-SPE, espera-se que esses resultados se apliquem também à primeira dessas técnicas.

Nota-se que os algoritmos de sincronização utilizados no experimento não foram projetados para operar com sinais criptografados. Portanto, há margem para reduzir a BER obtida. Uma das maneiras consideradas para implantar um algoritmo de sincronização para o caso de sinais criptografados é utilizar um piloto constituído por algumas dezenas de bits não criptografados. Os parâmetros utilizados para sincronizar este piloto seriam, então, aplicados ao sinal criptografado. Nosso grupo estava trabalhando nessa possibilidade quando houve a paralisação das atividades da universidade em consequência da pandemia de COVID-19.

Após a resolução do problema de sincronização, era esperado trafegar esses sinais criptografados por um ou mais enlaces constituídos por uma fibra seguida por um amplificador, cujo ganho é ajustado para compensar as perdas da fibra. Não é possível dizer de

antemão qual seria o comprimento do enlace a ser propagado, mas o laboratório utilizado dispõe de uma estrutura que permite fazer avaliações em comprimentos totais superiores a 2 mil km. A partir daí, outros algoritmos já implantados no receptor do laboratório seriam capazes de fazer a compensação de dispersão e outras operações necessárias para recuperação de sinais com detecção coerente.

Infelizmente, os resultados aprofundados desse experimento físico não puderam ser apresentados nesse trabalho. De fato, o grupo de pesquisa ainda tem intenção e trabalha para conseguir finalizá-los e, provavelmente, os resultados serão apresentados em trabalhos futuros de outros membros do grupo.

5 Conclusão

Todas as atividades de simulações previstas foram satisfatoriamente cumpridas e obtiveram resultados adequados. De fato, foi desenvolvido um código, atualmente incorporado ao KryptoSJ, que trata de sinais multiníveis de que quando modulados geram sinais QPSK ou 16-QAM. Nesse código, é possível utilizar técnicas de criptografia DSP-SPE, DSP-SPDE, DSP-SPE-Scr, dentre outras.

Os resultados obtidos em relação à segurança da nova técnica de criptografia são satisfatórios. Observa-se que a DSP-SPE-Scr oferece uma robustez maior a técnica de criptografia de dados mais utilizada no mundo (AES-256), mesmo trabalhando com um número consideravelmente baixo de fatias (BPSK em banda-base: 94 fatias, QPSK em banda-base:- 78 fatias, 16-QAM em banda-base: - 60 fatias). Também vimos que utilizar as operações de embaralhamento intracanal para aumentar a segurança é uma estratégia muito interessante porque essas operações não afetam o desempenho dos sinais em banda-base e aumentam a robustez a ataques de força bruta.

Os demais resultados obtidos também foram adequados. Comprovamos que as conversões óptico-elétrica e eletro-óptica, necessárias na DSP-SPE-Scr sobre sinais banda-base criptografados, não causam prejuízos significativos quando os valores de BER são altos. De fato, outros fatores de propagação, como o ruído, acabam sendo predominantes na degradação do sinal. Por isso, para esses casos a BER de um sinal que passou pelo processo de DSP-SPE-Scr é muito próxima à BER de um sinal que não passou por esse processo. Em relação a propagação de sinais criptografados, obtivemos um bom alcance considerando o limite da FEC. Apesar do sinal não criptografado conseguir um alcance de aproximadamente 160 km acima do sinal criptografado, este último ainda atende a redes metropolitanas com diâmetros maiores de 640 km. Adicionalmente, apesar desse trabalho ter considerado sempre uma abordagem válida para redes metropolitanas, enfatiza-se que a técnica estudada é válida para qualquer tipo de TON, incluindo enlaces submarinos e redes PONs.

Nossos resultados também indicaram que as propriedades de difusão e de confusão de Shannon e a segurança semântica não são satisfeitos quando uma única chave é usada para encriptar mais de um bloco de sinais. Por esse motivo, a estratégia de chaves dinâmicas foi adaptada para a técnica em questão. Verificou-se que esse novo esquema fez com que a

difusão, a confusão e a segurança semântica fossem atingidas, aumentando a segurança da DSP-SPE-Scr.

Por fim, notamos que uma das barreiras do experimento físico é manter a sincronização transmissor-receptor com o passar do tempo. Apesar de termos uma estratégia para esse problema, que é a ultilização de bits de pilotos não criptografados como cabeçalho, a paralização das atividades devido ao COVID-19 impossibilitou a geração de resultados a tempo da finalização desse trabalho. Contudo, o grupo de pesquisa está trabalhando com isso e os resultados serão provavelmente apresentados em trabalhos futuros de outros membros.

Ressaltamos que todos os resultados obtidos foram válidos para um paradigma de orientação à conexão. Porém, vale esclarecer que, se a orientação fosse a pacote, ainda assim os resultados seriam válidos. Nesse caso, o cabeçalho que contém a informação do endereço do pacote pode ser ou não encriptado. Caso esse cabeçalho seja encriptado, para manter o sigilo da comunicação, é importante que a chave usada seja diferente daquela utilizada com o nó de destino.

5.1 Lista de publicações e prêmio

A. Trabalhos Publicados

1. Abbade, M. L. F.; Nogueira, M. P.; Santos, M. O.; Fagotto, E. A. M.; Bonani, L. H.; Aldaya, I. DSP-based multi-channel spectral shuffling applied to optical networks. IEEE Photonics Technology Letters, v. 32, n. 3, p. 154–157, 2020.
2. 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.
3. de Andrade Bragagnolle, T.; Pereira Nogueira, M.; de Oliveira Santos, M.; do Prado, A. J.; Ferreira, A. A.; de Mello Fagotto, E. A.; Aldaya, I.; Abbade, M. L. F. All-optical spectral shuffling of signals traveling through different optical routes. In: 2019 21st International Conference on Transparent Optical Networks (ICTON). [S.l.: s.n.], 2019. p. 1–4. Trabalho convidado.

4. 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:2018 20th International Conference on Transparent Optical Networks (ICTON). 2018. p. 1–4. Trabalho convidado.

B. Trabalhos Aceitos

1. 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. Aceito como trabalho convidado em maio de 2020.
2. 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. Aceito como trabalho convidado em maio de 2020.

C. Trabalhos em Preparação

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

D. Prêmios

1. Quarta Colocada na Competição de Artigos de Estudantes no 2nd SBFoton International Optics and Photonics Conference. Sociedade Brasileira de Fotônica.

Referências[1]

Abbade, M. L. F.; Cvijetic, M.; Messani, C. A.; Alves, C. J.; Tenenbaum, S. All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys. *Appl. Opt.*, OSA, v. 54, n. 14, p. 4359–4365, May. Citado 3 vezes nas páginas 22, 23 e 38.

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: *2018 20th International Conference on Transparent Optical Networks (ICTON)*. [S.l.: s.n.], 2018. p. 1–4. Citado 2 vezes nas páginas 25 e 26.

Abbade, M. L. F.; Nogueira, M. P.; Santos, M. O.; Fagotto, E. A. M.; Bonani, L. H.; Aldaya, I. DSP-Based Multi-Channel Spectral Shuffling Applied to Optical Networks. *IEEE Photonics Technology Letters*, v. 32, n. 3, p. 154–157, 2020. Citado 2 vezes nas páginas 25 e 26.

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 . *11th Asian Photochemistry Conference - APC 2020*, Submetido em abril de 2020. Citado na página 26.

Agarwal, V.; Pareek, P.; Agarwal, M. Ultrafast Optical Message Encryption-Decryption System Using Semiconductor Optical Amplifier based XOR Logic Gate. In: *2018 International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD)*. [S.l.: s.n.], 2018. p. 65–66. Citado na página 22.

Agrawal, G. P. *Sistemas de Comunicação por Fibra Óptica*. 4ª. ed. [S.l.]: Elsevier, 2014. Citado 2 vezes nas páginas 29 e 53.

Chen, H.; Fang, A. W.; Peters, J. D.; Wang, Z.; Bovington, J.; Liang, D.; Bowers, J. E. Integrated microwave photonic filter on a hybrid silicon platform. *IEEE Transactions on Microwave Theory and Techniques*, v. 58, n. 11, p. 3213–3219, 2010. Citado na página 24.

Cornejo, J.; Tocnaye, J. L. de Bougrenet de la. Non-invasive WDM channel scrambling for secure high data rate optical transmissions. In: SHERIDAN, J. T.; WYROWSKI, F. (Ed.). *Photon Management III*. [S.l.]: SPIE, 2008. v. 6994, p. 124 – 131. Citado 2 vezes nas páginas 22 e 24.

Dahan, D.; Mahlab, U. Security threats and protection procedures for optical networks. *IET Optoelectronics*, v. 11, 05 2017. Citado 2 vezes nas páginas 20 e 22.

de Andrade Bragagnolle, T.; Pereira Nogueira, M.; de Oliveira Santos, M.; do Prado, A. J.; Ferreira, A. A.; de Mello Fagotto, E. A.; Aldaya, I.; Abbade, M. L. F. All-optical spectral shuffling of signals traveling through different optical routes. In: *2019 21st International Conference on Transparent Optical Networks (ICTON)*. [S.l.: s.n.], 2019. p. 1–4. Citado 2 vezes nas páginas 22 e 26.

Fips, N. *197: Announcing the Advanced Encryption Standard (AES)*. [S.l.]: Technol. Lab. Natl. Inst. Stand, 2009. 1–47 p. Citado na página 20.

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

Gayathri, J.; Subashini, S. A Survey on Security and Efficiency Issues in Chaotic Image Encryption. *Int. J. Inf. Comput. Secur.*, Inderscience Publishers, Geneva 15, CHE, v. 8, n. 4, p. 347–381, jan. 2016. Citado na página 21.

Iqbal, M. Z.; Fathallah, H.; Belhadj, N. Optical fiber tapping: Methods and precautions. *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, p. 164–168, 2011. 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 4 vezes nas páginas 28, 29, 36 e 38.

Liao, S.; Cai, W.; Liu, W.; Zhang, L.; Li, Y.; Ren, J.-G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.-P.; Li, F.-Z.; Chen, X.-W.; Sun, L.-H.; Jia, J.-J.; Wu, J.-C.; Jiang, X.-J.; Wang, J.-F.; Huang, Y.-M.; Wang, Q.; Zhou, Y.-L.; Deng, L.; Xi, T.; Ma, L.; Wang, X.-B.; Zhu, Z.-C.; Lu, C.-Y.; Shu, R.; Peng, C.-Z.; Wang, J.-Y.; Pan, J.-W. Satellite-to-ground quantum key distribution. *Nature 549*, p. 43–47, 2017. Citado na página 23.

Moizuddin, M.; Winston, J.; Qayyum, M. A comprehensive survey: Quantum cryptography. *2nd International Conference on Anti-Cyber Crimes (ICACC)*, p. 98–102, 2017. Citado na página 21.

Ngo, H. H.; Wu, X.; Le, P. D.; Wilson, C.; Srinivasan, B. Dynamic Key Cryptography and Applications. *International Journal of Network Security*, v. 10, n. 3, May 2010. Citado 2 vezes nas páginas 26 e 31.

Nogueira, M. P.; Abbade, M. L. Propagação de sinais ópticos criptografados por meio de embaralhamento espectral. 2019. Citado na página 25.

Pecora, L. M.; Carroll, T. L. Synchronization in chaotic systems. *Phys. Rev. Lett.*, American Physical Society, v. 64, p. 821–824, Feb 1990. Citado na página 21.

Pecora, L. M.; Carroll, T. L. Synchronization of chaotic systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, v. 25, n. 9, p. 097611, 2015. Citado na página 21.

Peng, Y.; Long, K.; Sun, Z.; Du, S. Propagation of all-optical crosstalk attack in transparent optical networks. *Optical Engineering*, SPIE, v. 50, n. 8, p. 1 – 5, 2011. Citado na página 20.

Pirandola, S.; Andersen, U. L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J.; Razavi, M.; Shaari, J. S.; Tomamichel, M.; Usenko, V. C.; Vallone, G.; Villoresi, P.; Wallden, P. Advances in Quantum Cryptography. *arXiv e-prints*, p. arXiv:1906.01645, jun. 2019. Citado na página 21.

Pizolato, J. C.; Romero, M. A.; Neto, L. G. Chaotic Communication Based on the Particle-in-a-Box Electronic Circuit. *IEEE Transactions on Circuits and Systems I: Regular Papers*, v. 55, n. 4, p. 1108–1115, 2008. Citado na página 21.

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. Citado 3 vezes nas páginas 22, 24 e 26.

Shafik, R. A.; Rahman, M. S.; Islam, A. R. On the Extended Relationships Among EVM, BER and SNR as Performance Metrics. In: *2006 International Conference on Electrical and Computer Engineering*. [S.l.: s.n.], 2006. p. 408–411. Citado na página 36.

Shaneman, K.; Gray, S. Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection and prevention. In: . [S.l.: s.n.], 2004. v. 2, p. 711 – 716 Vol. 2. Citado na página 20.

Shannon, C. E. Communication theory of secrecy systems*. *Bell System Technical Journal*, v. 28, n. 4, p. 656–715, 1949. Disponível em: ⟨https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1949.tb00928.x⟩. Citado na página 19.

Souza, W. S.; Abbade, M. L. Adaptação de Criptografia Espectral ao Paradigma do Advanced Encryption Standard. 2019. Citado 2 vezes nas páginas 25 e 55.

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*, Submetido em abril de 2020. Citado na página 26.

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 38.

Wei, H.; Zhang, C.; Wu, T.; Huang, H.; Qiu, K. Chaotic Multilevel Separated Encryption for Security Enhancement of OFDM-PON. *IEEE Access*, v. 7, p. 124452–124460, 2019. Citado na página 21.

Zhang, W.; Zhang, C.; Chen, C.; Zhang, H.; Jin, W.; Qiu, K. Hybrid chaotic confusion and diffusion for physical layer security in ofdm-pon. *IEEE Photonics Journal*, v. 9, n. 2, p. 1–10, 2017. Citado na página 25.

Zhao, A.; Jiang, N.; Liu, S.; Wang, Y.; Li, B.; Qiu, K. Secure Optical Communication in Fiber-Optical Systems Based on Physical Encryption of Synchronized Chaos. In: *2019 Asia Communications and Photonics Conference (ACP)*. [S.l.: s.n.], 2019. p. 1–3. Citado na página 21.

Zhao, A.; Jiang, N.; Liu, S.; Zhang, Y.; Qiu, K. Secure Optical Communication Based on Common-Injection-Induced Synchronization of Wideband Complex Signals. In: *2020 Optical Fiber Communications Conference and Exhibition (OFC)*. [S.l.: s.n.], 2020. p. 1–3. Citado na página 21.

Zou, X.; Li, M.; PaN, W.; YaN, L.; Azaña, J.; Yao, J. All-fiber optical filter with an ultranarrow and rectangular spectral response. *Opt. Lett.*, OSA, v. 38, n. 16, p. 3096–3098, Aug 2013. Citado na página 24.