RESSALVA

Atendendo solicitação do autor, o texto completo desta dissertação será disponibilizado somente a partir de 02/02/2024.

UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE ENGENHARIA - CÂMPUS DE SÃO JOÃO DA BOA VISTA
MESTRADO EM ENGENHARIA ELÉTRICA

PEDRO PAULO PARETO JUNIOR

DESENVOLVIMENTO EM LINGUAGEM PYTHON DE ALGORITMO PARA CRIPTOGRAFIA E DESCRIPTOGRAFIA DE SINAIS COM UTILIZAÇÃO DE CHAVES DINÂMICAS.

SÃO JOÃO DA BOA VISTA

2023

PEDRO PAULO PARETO JUNIOR

DESENVOLVIMENTO EM LINGUAGEM PYTHON DE ALGORITMO PARA CRIPTOGRAFIA E DESENCRIPTOGRAFIA DE SINAIS COM UTILIZAÇÃO DE CHAVES DINÂMICAS.

Trabalho de Mestrado apresentado à Universidade Estadual Paulista "Júlio de Mesquita Filho" como requisito para obtenção de título de Mestre em Engenharia Elétrica.

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade
Coorientador: Prof. Dr. Luiz Henrique Bonani do Nascimento

SÃO JOÃO DA BOA VISTA

2023

P228d

Pareto Junior, Pedro Paulo
Desenvolvimento em linguagem Python de algoritmo para criptografia e desencriptografia de sinais com utilização de chaves dinâmicas / Pedro Paulo Pareto Junior. -- São João da Boa Vista, 2023
87 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Engenharia, São João da Boa Vista
Orientador: Marcelo Luís Francisco Abbade
Coorientador: Luiz Henrique Bonani do Nascimento

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

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Fac uldade de Engenharia, São João da Boa Vista. Dados fornecidos pelo autor(a).

Impacto potencial desta pesquisa

Este trabalho aborda o tema de criptografia de sinais nos sistemas de comunicações nos meios de transmissão da Camada Física. Essa pesquisa estudou e analisou diversas técnicas de criptografia e desencriptografia de sinais, com propósito do aumento da segurança nesta camada. Entre elas destacamos as de embaralhamento intercanal com mais de 2 canais de entrada, e a técnica de utilização de chaves dinâmicas na transmissão de blocos de mensagens. Sendo que neste trabalho essas duas técnicas foram implementadas e testadas com uso da linguagem Python.

Potential impact of this research

This work addresses the topic of signal encryption in communications systems in Physical Layer transmission media. This research studied and analyzed several signal encryption and decryption techniques, with the aim of increasing security at this layer. Among them we highlight interchannel shuffling with more than 2 input channels, and the technique of using dynamic keys in the transmission of message blocks. In this work, these two techniques were implemented and tested using the Python language.

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: Desenvolvimento em linguagem Python de algoritmo de chaves dinâmicas para criptografia e desencriptografia de sinais

AUTOR: PEDRO PAULO PARETO JUNIOR

ORIENTADOR: MARCELO LUÍS FRANCISCO ABBADE

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

Prof. Dr. MARCELO LUÍS FRANCISCO ABBADE (Participaçao Virtual)
Departamento de Engenharia Eletronica e de Telecomunicacoes / Faculdade de Engenharia de Sao Joao da Boa Vista UNESP

Prof. Dr. IVAN ARITZ ALDAYA GARDE (Participaçao Virtual)
Departamento de Engenharia Eletronica e de Telecomunicacoes / Faculdade de Engenharia de Sao Joao da Boa Vista UNESP

Prof. Dr. MARCELO ZANOTELLO (Participaçao Virtual)
Centro de Ciências Naturais e Humanas / Universidade Federal do ABC

São João da Boa Vista, 01 de agosto de 2023

Verônica Liberali Messias
Supervisora Técnica de Seção
Seção Técnica de Graduação e Pós-Graduação

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE ENGENHARIA - CAMPUS DE SOROCABA MESTRADO EM ENGENHARIA ELÉTRICA

TRABALHO DE MESTRADO

DESENVOLVIMENTO EM LINGUAGEM PYTHON DE ALGORITMO PARA CRIPTOGRAFIA E DESCRIPTOGRAFIA DE SINAIS COM UTILIZAÇÃO DE CHAVES DINÂMICAS.

Aluno: Pedro Paulo Pareto Junior
Orientador: Prof. Dr. Marcelo Luís Francisco Abbade
Coorientador: Prof. Dr. Luiz Henrique Bonani do Nascimento

Banca Examinadora:

- Marcelo Luís Francisco Abbade (Orientador)
- Ivan Aritz Aldaya Garde (Examinador)
- Marcelo Zanotello (Examinador)

São João da Boa Vista, 01 de Julho de 2023

Dedicatória

Dedico este trabalho a minha esposa, as minhas filhas, meus amigos, professores, funcionários e ao companheiro de pesquisa Ivan, que contribuíram com meu desenvolvimentopessoal, profissional e pelo carinho e auxílioque obtive durante todo o meu período acadêmico.

AGRADECIMENTOS

Agradeço a minha esposa por ajudar a me tornar uma pessoa melhor e uma excelente companheira nas reflexões e decisões em vários momentos importantes durante a minha vida.

As minhas filhas Gabriela Maia Pareto e Rafaela Maia Pareto que foram e são fontes de energia para alimentar minha persistência e inspiração, pois para nossos filhos o melhor legado que podemos deixar são exemplos, ações e pensamentos.

Ao meu orientador de pesquisa, Prof. Dr. Marcelo Luís Francisco Abbade, por ter me aceitado na equipe de pesquisa, pela paciência, por ter me inspirado em meu desenvolvimento pessoal e profissional, e especialmente pela sábia orientação na realização deste Trabalho de Mestrado.

Ao meu coorientador Luiz Henrique Bonani por todo o apoio e ensinamentos, o qual ajudou com suas orientações à este trabalho. Também agradeço a todos os outros professores que tive prazer de cursar suas disciplinas.

Ao meu colega de pesquisa Ivan Eduardo Lage Rodrigues, que colaborou para que o nosso trabalho em equipe sempre fosse de ajuda mútua na busca de soluções e de novas ideias.

“Quanto mais estudo mais sinto que minha mente nisso é insaciável”

(Augusta Ada Byron King, Condessa de Lovelace)

RESUMO

A criptografia de sinais é um processo de transformação das propriedades físicas dos sinais, tornando os sinais originais em sinais indecifráveis para quem não possui o algoritmo de desencriptação. Esta criptografia é realizada na Camada Física, e seu propósito consiste no aumento da segurança nesta camada dos sistemas de comunicações. Neste processo de encriptação o agente transmissor transforma o sinal original por meio de um algoritmo e de uma chave de encriptação. Enquanto o agente receptor poderá ter acesso ao sinal original por meio do processamento do algoritmo de desencriptação utilizando uma chave como entrada neste algoritmo.

Nosso grupo escolheu a linguagem Python para simular criptografia de sinais, por ser de alto nível, multiplataforma, orientada a objetos, estruturada, com vasta e crescente biblioteca de funções, e gratuita. Podendo ser executada em qualquer sistema operacional por ser interpretada, além de permitir criação de classes com seus respectivos objetos.

O objetivo deste trabalho foi implementar alguns dos módulos utilizados para este simulador e colaborar na implementação de outros. As principais contribuições deste trabalho foram as implementações do módulo de embaralhamento intercanal e o de chaves dinâmicas.

O módulo de embaralhamento intercanal realiza o troca de amostras entre diferentes sinais presentes na entrada do simulador. Neste algoritmo há uma chave que vai promover a troca das amostras espectrais entre estes diferentes sinais, e esta chave é gerada por uma distribuição aleatória discreta das amostras. A chave que contêm a sequência do embaralhamento, será utilizada pelo receptor por meio de um algoritmo de desencriptação para realizar o desembaralhamento, e ter acesso à informação original. O resultado alcançado foi o mesmo gráfico dos valores de BER em função da SNR obtido pelo algoritmo em MatLab®.

O objetivo do módulo das chaves dinâmicas foi de encriptar cada bloco de informação com uma chave distinta ao longo do tempo de forma dinâmica e automática para cada nova transmissão. Neste trabalho de maneira complementar foi implementado o algoritmo das chaves dinâmicas para a encriptação e desencriptação espectral de fase com processamento digital do sinal (*spectral phase digital signal processing*, SPE-DSP). O processamento deste algoritmo executa operações com manipulações de matrizes e vetores, através da utilização de várias funções auxiliares, para a geração das chaves dinâmicas. Este módulo foi integrado ao algoritmo de criptografia e descriptografia chamado simulador KryptoSJPy. Os resultados obtidos comprovam que a utilização das chaves dinâmicas na encriptação das mensagens atende as propriedades de difusão e confusão propostas por Shannon. Outro resultado foi que a comparação dos valores das chaves dinâmicas obtidas com o algoritmo das chaves dinâmicas realizados em MatLab® e em Python apresentou um desvio percentual igual a zero.

Palavras–chave: Criptografia de sinais, chaves dinâmicas, embaralhamento intercanal, arquitetura de algoritmo, encriptação espectral de fase, Python.

Signal encryption is a process of transforming the physical properties of signals, turning the original signals into indecipherable signals for those who do not have the decryption algorithm. This encryption is performed at the physical layer, and its purpose is to increase security at this layer of communication systems. In this encryption process, the transmitting agent transforms the original signal using an algorithm and an encryption key. While the receiving agent may have access to the original signal through the processing of the decryption algorithm using a key as input in this algorithm.

Our group chose the Python language to simulate signal encryption because it is high-level, cross-platform, object-oriented, structured, with a vast and growing library of functions, and free. It can be executed in any operating system because it is interpreted, in addition to allowing the creation of classes with their respective objects.

The objective of this job was to implement some of the modules used for this simulator and collaborate in the implementation of others. The main contributions of this job were the implementations of the interchannel scrambling and the dynamic keys.

The interchannel scrambling module performs the exchange of samples between different signals present at the simulator input. In this algorithm there is a key that will promote the exchange of spectral samples between these different signals, and this key is generated by a discrete random distribution of the samples. The key containing the scrambling sequence will be used by the receiver through a decryption algorithm to perform the unscrambling and have access to the original information. The result achieved was the same graph of BER and SNR obtained by the algorithm in MatLab®.

The objective of the dynamic keys' module was to encrypt each block of information dynamically and automatically with a different key over time for each new transmission. In this job, in a complementary way, the algorithm of dynamic keys for phase spectral encryption and decryption with digital signal processing (spectral phase digital signal processing, SPE-DSP) was implemented. The processing of this algorithm performs operations with manipulations of matrices and vectors, by several auxiliary functions, for the generation of dynamic keys. This module has been integrated into the encryption and decryption algorithm called the KryptoSJPy simulator. The obtained results prove that the use of dynamic keys in the encryption of messages meets the properties of diffusion and confusion proposed by Shannon. Another result was that the comparison of the dynamic keys values obtained with the dynamic keys algorithm performed in MatLab® and in Python presented a percentage deviation equal to zero.

Keywords: Signal encryption, dynamic keys, interchannel scrambling, algorithm architecture, phase spectral encryption, Python.

Lista de figuras

Lista de tabelas

Lista de abreviações e siglas

AWGN	*Additive white Gaussian noise*
AES	*Advanced Encryption Standard* (Padrão de criptografia avançado)
BER	*Bit error ratio* (Taxa de erro de bit)
BPSK	*Binary phase shift keying* (Modulação por deslocamento de fase binária)
DSP	*Digital signal processing* (Processamento digital de sinais)
DK	*Key Dinamic* (Chave dinâmica)
FEC	*Forward error correction* (Correção de erros antecipada)
FFT	*Fast Fourier transform* (Transformada rápida de Fourier)
IDE	*Integrated development environment* (Ambiente de Desenvolvimento Integrado)
iFFT	*Inverse fast Fourier transform* (Transformada rápida inversa de Fourier)
MVC	Modelo-visão-controlador
OSI	Open Systems Interconnection
PEP	*Python Enhancement Proposals* (Propostas de Enriquecimento do Python)
PRBS	*Pseudo-Random Bit Sequence* (Sequência de bits pseudoaleatória)
PSF	*Python Software Foundation* (Fundação de Software de Python)
QAM	*Quadrature amplitude modulation* (Modulação de amplitude em quadratura)
QKD	*Quantum Key Distribution* (Distribuição de Chave Quântica)
QPSK	*Quadrature phase shift keying* (Modulação por deslocamento de fase em quadratura)
RCF	*Raised Cosine Filter* (Filtro de Cosseno Levantado)
Scr	*Scrambling* (Embaralhamento Intracanal)
SER	*Symbol Error Rate* (Taxa de Erro de Símbolo)
SLM	*Spatial light modulator* (Modulador espacial de luz)
SNR	*Signal-noise ratio* (Razão sinal-ruído)
SPE	*Spectral Phase Encoding* (Codificação espectral por fase)

Lista de símbolos

n_{aps}	Número de amostras por símbolo
n	Numero de amostras do sinal
N_s	Número de símbolos
$s[n]$	Sinal digital complexo
B	Banda do sinal
R_s	Taxa de símbolos
r	Fator de roll-off
P_{noise}	Potência do ruído
σ_n^2	Variância do ruído
$\sigma_{n_{re}}^2$	Variância do ruído que ocorre na componente real do sinal
$\sigma_{n_{im}}^2$	Variância do ruído que ocorre na componente imaginária do sinal
P_{signal}	Potência do sinal
$\sigma_{s[k]}^2$	Variância do sinal
SNR_{dB}	Razão sinal-ruído em dB
Φ_{n}	Fase aleatória da n-ésima amostra do sinal
$C[n]$	Sinal criptografado
k_f	Chave do sistema encriptado por SPE
k_s	Chave do sistema encriptado por Scr
k_t	Chave temporária
k_i	Chave inicial
k_s	Chave semente
D_{K1}	Primeiro bloco da chave dinâmica
D_{K2}	Segundo bloco da chave dinâmica
D_{Kn}	*n* bloco da chave dinâmica
M	Quantidade de simbolos
Q	Função Q

Sumário

1. Introdução

1.1 Sistemas de comunicações sem fio e utilização de rede ópticas

No caso de sistemas de comunicações sem fio por rádio frequências temos as comunicações móveis celulares. Atualmente as tecnologias empregadas nas redes de comunicação móveis celulares passam por grandes avanços tecnológicos. Entre eles podemos citar a tecnologia Evolução de Logo Prazo(*Long Term Evolution Advanced* - LTE A), chamada de quarta geração, e que alcança em laboratórios 300 Mbps e com tempo de latência de aproximadamente 20 milissegundos. Há ainda uma tecnologia mais recente chamada de quinta geração (5G), que já começou a ser implantada no mundo, e até 2025 possuirá aproximadamente 26% de todas as conexões móveis celulares do mundo conforme mencionado no documento da GSMA [1].

A tecnologia do 5G pode alcançar velocidades de 20 Gbps conforme o artigo de Pant [2] outra característica importante associada ao 5G é o tempo de latência que varia entre 1 e 10 milissegundos.

As redes celulares móveis com emprego de tecnologias LTE e 5G possibilitam a utilização de altas taxas de velocidade de dados em comparação com tecnologias empregadas em gerações anteriores do sistema móvel celular. Devido ao incremento de uma maior demanda de dados da rede celular com as tecnologias LTE e 5G, há a necessidade de uma rede de transmissão de sinais de maior velocidade e de maior capacidade, para permitir uma eficiente interconexão dos usuários móveis celulares com as redes de Internet, e de outras redes comerciais púbicas ou privadas. Com isto as conexões passaram a utilizar backbones ópticos de maior capacidade. No caso do 5G, a conexão dos equipamentos de irradiação dos sinais de rádio frequência com a rede de transmissão, passaram a ser quase que exclusivamente por fibra óptica. Isto foi necessário para suprir novos usuários com alta taxa de dados, tanto para receber das estações celulares 5G, como para transmitir para as estações celulares. Atualmente os meios de transmissão das redes móveis 5G, em função da necessidade da alto volume de dados transmitidos e recebidos, dependem do entroncamento com a rede óptica, que passou a ser cada vez mais utilizada na infraestrutura destes sistemas móveis celulares.

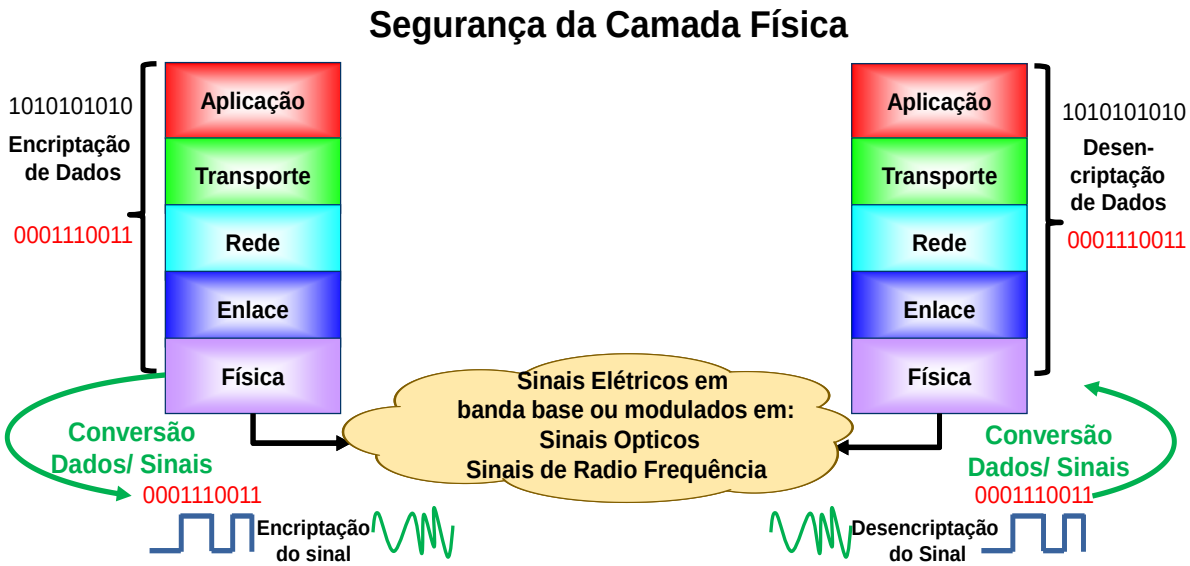
As redes ópticas também tem registrado grandes avanços tecnológicos permitindo maior capacidade e velocidade nas transmissões. Em 2021 um teste em um centro de pesquisa do Japão [3] alcançou 319 Terabits por segundo(Tb/s).

Estes avanços tecnológicos nos sistemas móveis celulares e na rede óptica, juntamente com o incremento de usuários importantes em segmentos corporativos, governamentais, militares etc., aumentaram o interesse por segurança nas comunicações. Como indicado na Figura 1.1, há mecanismos comerciais para implantação de confidencialidade nas camadas superiores de arquitetura hierárquicas de sistemas de telecomunicações. No entanto, a Camada Física, responsável por converter dados (bits) para sinais, ainda não dispõe destes mecanismos e, no melhor do nosso conhecimento, a criptografia realizada na Camada Física ainda está a nível de pesquisa. Este tipo de criptografia é chamado neste texto de criptografia de sinal.

A criptografia de sinal é um processo de transformação das propriedades físicas dos sinais. Neste processo, um transmissor converte o sinal original, por meio de um algoritmo e de uma chave de encriptação, para o sinal criptografado. Por sua vez, o receptor pode recuperar o sinal original, utilizando um algoritmo de desencriptação com uma chave adequada. Receptores que não possuam estas chaves não poderão recuperar o sinal original. A criptografia de sinal será explicada em detalhes no Capítulo 3.

Nosso grupo de pesquisa está desenvolvendo um software, para implementar a criptografia de sinais por meio de simulações com a linguagem Python. Este software é chamado de KryptoSJPy. O objetivo deste trabalho foi implementar alguns dos módulos utilizados para o simulador KryptoSJPy e colaborar na implementação de outros módulos. As principais contribuições deste trabalho foram as implementações do módulo de embaralhamento intercanal e o de chaves dinâmicas, que serão detalhadas ao longo deste trabalho. A pesquisa sobre criptografia objeto deste trabalho, poderá ajudar no futuro empresas de telecomunicações aprimorar a segurança dos sinais providos a seus clientes.

Figura 1.1 Ilustração de criptografia na Camada Física do modelo TCP-IP.



Fonte M. L. F. Abbade; I.E.L.Rodrigues ; P.P.Pareto.J; W.S.Souza ; L. H. Bonani ; I. Aldaya . in 2021 SBFoton International Optics and Photonics Conference, SBFoton IOPC 2021, 2021.

A importância dos módulos de embaralhamento intercanal e de chaves dinâmicas, que serão explicadas ao longo deste trabalho, estão relacionadas com a criptografia para mais de dois sinais de entrada no simulador e na confidencialidade das informações transmitidas, respectivamente.

No próximo Capítulo 2 serão explicados o que é a criptografia de dados e as técnicas existentes, que operam nas camadas superiores de arquitetura hierárquicas dos sistemas de comunicação conforme apresentado na ilustração da Fig. 1.1.

6. CONCLUSÃO

Este trabalho teve como propósito apresentar minhas principais contribuições ao software de criptografia de sinais KryptoSJPy, além de colaborar na implementação de outros. As principais contribuições deste trabalho foram as implementações do módulo de embaralhamento intercanal e o módulo de chaves dinâmicas.

A implementação do módulo de embaralhamento intercanal foi testada para 2, 4, e 8 canais para BPSK, QPSK e 16QAM, com resultados aproximadamente os mesmos sem encriptação e com encriptação SPE, conforme apresentado nos gráficos de BER e SNR do Cap. 5. Nos gráficos da BER e SNR verificamos que para BPSK, QPSK e 16QAM, um alto valor de BER está associado a um baixo valor de SNR e limitado a um valor de 0,5 de BER. Os sinais encriptados não podem ser recuperados com valores de BER menor do que 0.5. Nestes gráficos também podemos concluir que o sinal BPSK em comparação com os sinais transmitidos em QPSK e 16QAM, foi o que apresentou menor valor de SNR com BER próximo do limite da FEC, podendo sua transmissão alcançar maiores distâncias com recuperação dos sinal.

Este trabalho tratou principalmente da implementação do módulo de geração das chaves dinâmicas desenvolvido na linguagem Python com encriptação por fases. Neste módulo de geração das chaves podemos destacar a função ”*whirlpool”*, que utiliza a função de compressão Miyaguchi- Preneel nos dados gerados no processo de substituição e permutação, conforme apresentado no Cap. 4. Esta função de compressão Miyaguchi-Preneel é uma das diferenças entre o algoritmo da função ”*whirlpool”* em comparação com a função AES, e esta diferença também contribui para que o número de interações na função ”*whirlpool”* seja igual a 10, enquanto na função AES com 256 bits utiliza o número de interações R igual a 14, causando redução do tempo de processamento desta função e no tempo de processamento do módulo das chaves dinâmicas.

No algoritmo do módulo das chaves dinâmicas uma sugestão de análise para melhoria da segurança seria na função secundária “*buildconstants”*. Esta função é a responsável pela geração das constantes C e rc, e a obtenção destas constantes depende diretamente do bloco de caracteres chamado de *sbox*,

definido por 512 caracteres. Este conjunto de caracteres poderiam ser substituídos de tempos em tempos, causando mudança nas constantes C e rc, dificultando ainda mais a tarefa de descoberta das chaves por um possível intruso, que tente utilizar estratégias eficientes de desencriptação da mensagem.

Neste trabalho também foram verificados os mesmos resultados obtidos com o simulador de criptografia de sinais Kryptos_sj em MatLab®, para os gráficos do diagrama de constelação para BPSK, QPSK e 16QAM. As monitorações foram realizadas em vários pontos do percurso do sinal, passando pelos módulos do transmissor, canal AWGN, e do módulo receptor do software KryptoSJPy.

A performance de qualidade dos sinais sem encriptação e com encriptação no KryptoSJPy, apresentaram bons resultados e de acordo com esperado. Foram realizadas simulações com variação do desvio padrão de ruído gaussiano de $\boldsymbol{\sigma}$ = 0,16 à $\boldsymbol{\sigma}$ = 0,32 apresentados nos diagramas de constelação do Cap. 5. Foi verificado no módulo receptor, que para sinais sem encriptação, ocorreu aumento da mancha das amplitudes nos eixos I e Q, mas sem a sobreposição dos símbolos. Para os sinais encriptados SPE com a variação do desvio padrão de ruído gaussiano os diagramas de constelação para BPSK, QPSK e 16QAM, causaram uma mancha circular sem identificação dos símbolos nos eixos I e Q, mas no receptor após a desencriptação os sinais foram recuperados, e sem sobreposição dos símbolos nos eixos I e Q de acordo com o esperado.

Foram realizados testes de segurança, para certificar que foram atendidas as propriedades de difusão e confusão, conforme verificado na simulação de criptografia de sinais nos resultados apresentados no Cap. 5.

Para o teste da difusão foi confirmado que a alteração de 1 bit da mensagem causou a alteração de aproximadamente 50% dos bits da mensagem encriptada. No caso do teste da confusão a alteração de 1 bit da chave dinâmica, causou a alteração de aproximadamente 50% da mensagem encriptada. Caso não houvesse utilização das chaves dinâmicas a alteração dos bits da mensagem seria de apenas 5%. Comprovou-se que o uso das chaves dinâmicas, é essencial para criptografia de sinais, alcançando valores aproximados de 50% de diferença dos bits transmitidos, impedindo a

desencriptação da mensagem original e sem nenhum prejuizo tecnico na trasnmissão das mensagens.

Foi verificado que os valores obtidos na geração das chaves dinâmicas realizadas em Python, foram os mesmos valores obtidos para o algoritmo desenvolvido pelo nosso grupo de pesquisa em MatLab®. Para esta comparação foi utilizada o mesmo conjunto de dados de entrada, que foi utilizada no algoritmo em MatLab®. Adicionalmente também foram realizadas comparações destes valores com diversos comprimentos de chaves.

Uma sugestão de continuidade deste trabalho seria avaliação de uma estratégia de embaralhamento para dois ou mais sinais de entrada, combinando a técnica de embaralhamento intracanal e de embaralhamento intercanal com a troca entre diferentes posições das amostras em cada um dos sinais, e na sequência realizando o embaralhamento entre as amostras dos sinais de entrada conforme a Fig. 6.1.

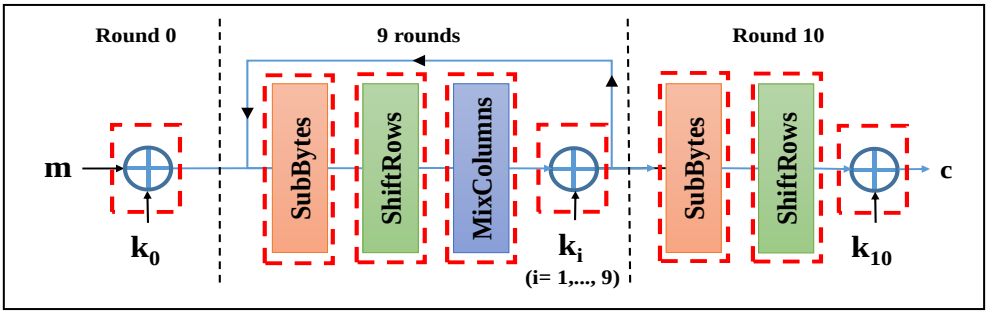
Fig.6.1 Ilustração de nova estratégia de embaralhamento acima de 2 canais.

Posição	sinal A	sinal B
1	3	37
2	5	12
3	8	3
4	27	15
5	67	77

Fonte autoria própria,2023

Outra sugestão seria analisar se é possível aumentar ainda mais a segurança do algoritmo da função ”*whirlpool*”, analisando os blocos do processamento de substituição e permutação de bits para a geração de 512 bits desta função hash, conforme a Fig. 6.2.

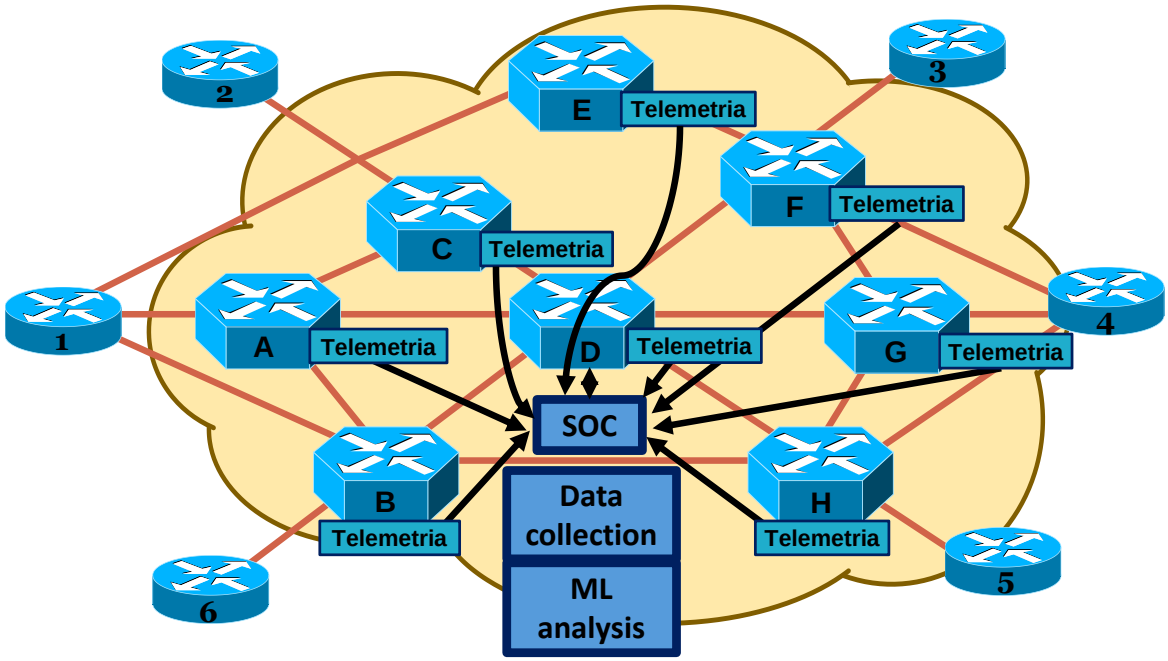
Fig.6.2 Ilustração de nova estratégia de aumento de segurança do bloco da função ”*whirlpool*”.



Fonte M. L. F. Abbade; I.E.L.Rodrigues ; P.P.Pareto.J; W.S.Souza ; L. H. Bonani ; I. Aldaya . in 2021 SBFoton International Optics and Photonics Conference, SBFoton IOPC 2021, 2021.

Uma sugestão de expansão deste trabalho seria a integração com módulos de "*machine learning*" [45],[46],[47],[48],[49], especificamente o de classificação por algoritmo de rede neural e o de árvore de decisão. Seria uma sugestão visando a monitoração da integridade da operação de uma rede óptica [50]-[51] com e sem utilização de criptografia de sinais, conforme a ilustração da Fig. 6.3.

Fig. 6.3 Ilustração de uma estratégia utilizando *Machine Learning* e com uso de telemetria.



Fonte M. L. F. Abbade; I.E.L.Rodrigues ; P.P.Pareto.J; W.S.Souza ; L. H. Bonani ; I. Aldaya . in 2021 SBFoton International Optics and Photonics Conference, SBFoton IOPC 2021, 2021.

REFERÊNCIAS

[1] GSM Association. Availble: https://www.gsma.com/futurenetworks/ip_services/understanding-5g/ (Current 2023, Jun.15).

[2] M. Pant and L. Malviya, "**Design developments and applications of 5G antennas: A review**", *International J. of Microwave and Wireless Technologies*, pp. 1-27, 2022.

[3] Benjamin J. Puttnam et all, "**Demonstration of World Record: 319 Tb/s Transmission over 3,001 km with 4-core optical fiber**", National Institute of Information and Communications Technology. Availble: https://www.nict.go.jp/en/press/2021/07/12-1.html (Current 2022, Oct.03).

[4] PAAR, C.; PELZL, J. **Understanding Cryptography: A Textbook for Students and Practitioners**. 2nd. ed. rev. Heidelberg: Springer-Verlag Berlin Heidelberg, 2010. v. 372. ISBN 978-3-642-04101-3. DOI 10.1007/978-3-642-04101-3. Disponível em: https://link.springer.com/book/10.1007%2F978-3-642-04101-3.

[5] J. Katz and Y. Lindell, **Introduction to Modern Cryptography**, 2nd ed. Chapman and Hall/ CRC, 2014.

[6] M. E. Hellman and D. Whitfield**, "New Directions in Cryptography,"** IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, 1976.

[7] Menezes, A.J., van Oorschot, P.C., & Vanstone, S.A. (1997). **Handbook of Applied Cryptography** (1st ed.). CRC Press. https://doi.org/10.1201/9780429466335

[8] GUTMANN, P. **Cryptographic Security Architecture**. 1st. ed. New York, USA: Springer, 2004. 320 p. ISBN 978-0-387-21551-8. Disponível em: https://link.springer.com/book/10.1007/b97264#about.

[9] Ngo, Huy Hoang et al. "**Dynamic Key Cryptography and Applications**." Int. J. Netw. Secur. 10 (2010): 161-174.

[10] R. L. Rivest, A. Shamir, and L. M. Adleman, **"A method for obtaining digital signatures and public key cryptosystems,"** Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[11] SINGH, G., **"A study of encryption algorithms (rsa, des, 3des and aes) for information security,"** International Journal of Computer Applications,

Foundation of Computer Science, v. 67, n. 19, 2013

[12] S. Paine, **Criptografia e Segurança - O Guia oficial RSA**. Campus, 2002.

[13] SANTOS, M. O. et al. All- "**Optical Spectral Shuffling Applied to 16-QAM Signals,"** 2019 SBFoton International Optics and Photonics Conference, São Paulo, Outubro 2019. DOI 10.1109/SBFoton-IOPC.2019.8910255. Disponível em: https://ieeexplore.ieee.org/document/8910255.

[14] C. Shannon, **"Communication theory of secrecy systems,"** Bells Systems Technical Journal, no. 4, 1949.

[15] A. Berent, **"AES (advanced encryption standard) simplified,"** tech. rep., ABI Software Development, 2003.

[16] NIST, **"Advanced encryption standard (AES),"** tech. rep., National Institute of Standards and Technology NIST. Federal Information Processing Standards Publication 197.

[17] M. L. F. Abbade, M. P. Nogueira, M. O. Santos, E. A. M. Fagotto, L. H. Bonani, and I. Aldaya, **"DSP-Based Multi-Channel Spectral Shuffling Applied to Optical Networks,"** IEEE Photonics Technol. Lett., vol. 32, no. 3, pp. 154–157, 2020.

[18] KARTALOPOULOS, S. V. **"Quantum Cryptography for Secure Optical Networks**. **IEEE International Conference on Communications,"** p. 1311-1316, 2007. Disponivel em: 10.1109/ICC.2007.221.

[19] PESSOA JÚNIOR, Osvaldo. Conceitos de Física Quântica, Ed. Livraria da Física, São Paulo, SP, 2003.

[20] SULZBACH, Jaime André. **"Análise de viabilidade de Criptografia Quântica"**, Univ. Do Vale do Rio dos Sinos, São Leopoldo, RS, 2003.

[21] B. Lydia, B. Smail and S. Mohamed, "**Application of quantum cryptography in an optical link,**" 2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B), Boumerdes, Algeria, 2017, pp. 1-5, doi: 10.1109/ICEE-B.2017.8192039.

[22] G. Gordon, and G. Rigolin, Opt. Commun. 283, 184 (2010).

[23] EKERT, A. **"Quantum Cryptography based on Bell's Theorem Physical,"** Review Letters, v. 67, n. 6, Aug.1991.

[24] BENNETT, C. **"Quantum Cryptography Using Any Two Nonorthogonal States,"** Physical Review Letters, v. 68, n. 21, p. 3121-3124, May.1992.

[25] C.Bennett and G. Brassard , **Quantum cryptography, Public key distribution and coin tossing**, Proc. of the Int. Conf. Comp. Syst. and Signal Proc , Bangalore, 1984, pp.175.

[26] De Oliveira, Luiz P.L., and Marcelo Sobottka. **"Cryptography with Chaotic Mixing,"** Chaos, Solitons and Fractals 35.3 (2008): 466-71. Web.

[27] S. Li, X. Mou, Z. Ji, J. Zhang, and Y. Cai, **"Performance analysis of jakimoski-kocarev attack on a class of chaotic cryptosystems,"** Physics Letters A, vol. 307, no. 1, pp. 22–28, 2003.

[28] VEENUS, P. K. et al. The implementation of chaotic encryption scheme for images. In: "**2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT),"** IEEE, 2015. p. 588-592.

[29] G. Alvarez, G. Monotoya, and M. Romera, **"Chaotic cryptosystems,"** Proc. IEEE 33rd Annual Int. Carnahan Conf. Security Technology, pp. 332–338, 1999.

[30] Li, Shujun, et al. **Problems with a probabilistic encryption scheme based on chaotic systems, accepted by Int.** J. Bifurcation and Chaos. 2003.

[31] CORNEJO, J.; TOCNAYE, E. L. M. B. "**Non-invasive WDM channel scrambling for secure high data rate optical transmissions,"** Proc. SPIE: Photon Management III, Strasbourg, France, v. 6994, Abril 2008. DOI 10.1117/12.781036. Disponível em: https://www.spiedigitallibrary.org/conference-proceedings-of-spie.

[32] M. S. Baptista, **"Cryptography with chaos,"** Physics Letters A, no. 240, pp. 50–54, 1998.

[33] E. Biham and A. Shamir, **Differential cryptanalysis of the data encryption standard**. London, UK: Springer-Verlag, 1993.

[34] A. Biryukov and D. Wagner**, "Advanced slide attacks,"** Advances i Cryptology EUROCRYPT 2000, no. 1807, pp. 589–606, 2000.

[35] Alligood, Kathleen T., et al. "**Chaos: an introduction to dynamical systems.**" *SIAM Review* 40.3 (1998): 732-732.

[36] S. Li, G. Chen, K. Wong, X. Mou, and Y. Cai, **"Baptista-type chaotic cryptosystems: problems and countermeasures,"** Physics Letters A, no. 332, pp. 368–375, 2004.

[37] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, **"Cryptanalysis of**

an ergotic chaotic cipher," Physics Letters A, no. 311, pp. 172–179, 2003.
[38] SANTOS, M. **Criptografia na Camada Física Baseada em Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas.** Tese (Mestrado em Engenharia Elétrica) - Engenharia Elétrica pelo Programa de Pós-graduação em Engenharia Elétrica, Universidade Estadual Paulista Júlio de Mesquita Filho - Câmpus de São João da Boa Vista,2020.
[39] BRAGAGNOLLE, A. *et al.* **"All-Optical Spectral Shuffling of Signals Traveling through Different Optical Routes,"** 2019 21st International Conference on Transparent Optical Networks (ICTON). (S.l.): (s.n.). 2019. p. 1-4. DOI:10.1109/ICTON.2019.8840243.
[40] SOUZA, W. S. *et al.* **"Spectral Shuffling with Phase Encoding and Dynamic Keys Applied to Transparent Optical Network Signals,"** 2020 22nd International Conference on Transparent Optical Networks (ICTON). (S.l.): (s.n.). 2020. p. 1-4. DOI:10.1109/ICTON51198.2020.9203374.
[41] Abbade, Marcelo & Junior, Pedro & Rodrigues, Ivan & Souza, Welerson & Bonani, Luiz & Aldaya, Ivan. (2021). **"Security in Optical Communication Systems: Data Encryption and Beyond,"** 1-6. 10.1109/SBFotonIOPC50774.2021.9461932.
[42] ABBADE, M. L. F. et al. All-**optical cryptography of M-QAM formats byusing two-dimensional spectrally sliced keys**. Applied Optics. , v. 54, nº 14, pg. 4359-4365. May. 2015. Disponível em: https://osapublishing.ez87.periodicos.capes.gov.br/ao/abstract.cfm?uri=ao-54-14-4359.
[43] LATHI, B. P.; DING, Z. **Modern Digital and Analog Communication Systems**. 4th ed. p. cm. ISBN 978-0-19-538493-2 (hardcover: alk. paper). citado em página 850.
[44] Akihiro Shimizu, Shoji Miyaguchi - Fast Data Encipherment Algorithm FEAL. Advances in Cryptology — EUROCRYPT' 87. Workshop on the Theory and Application of Cryptographic Techniques Amsterdam, The Netherlands, April 13–15, 1987 Proceedings. Springer Berlin Heidelberg. 1988. Section VI: pp 267-278. ISBN: 978-3-540-19102-5, 978-3-540-39118-0.
[45] K. Shaneman and S. Gray, **"Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention,"** Proc. - IEEE Mil. Commun. Conf. MILCOM, vol. 2, pp. 711–716,

2004.

[46] C. Natalino, M. Schiano, A. Di Giglio, L. Wosinska, and M. Furdek, **“Experimental Study of Machine-Learning-Based Detection and Identification of Physical-Layer Attacks in Optical Networks,”** J. Light. Technol., vol. 37, no. 16, pp. 4173–4182, 2019.

[47] M. Bensalem, S. K. Singh, and A. Jukan**, “On detecting and preventing jamming attacks with machine learning in optical networks,”** in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1–6.

[48] M. Furdek, C. Natalino, A. Di Giglio, and M. Schiano**, “Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats (Invited),”** J. Opt. Commun. Netw., vol. 13, no. 2, pp. A144–A155, 2021.

[49] Y. Li et al., **“Optical spectrum feature analysis and recognition for optical network security with machine learning,”** Opt. Express, vol. 27, no. 17, p. 24808, 2019.

[50] RAHOUMA, K.; ALI, A. “**Applying Intrusion Detection and Response systems for securing the Client Data Signals in the Egyptian Optical Network,”** Procedia Computer Science, v. 163, p. 538–549, 2019.

[51] M. Zafar Iqbal, H. Fathallah, and N. Belhadj, **“Optical fiber tapping: Methods and precautions,”** 8th Int. Conf. High-Capacity Opt. Networks Emerg. Technol. HONET 2011, pp. 164–168, 2011.