



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ
IFCE *CAMPUS* FORTALEZA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELECOMUNICAÇÕES
MESTRADO ACADÊMICO EM ENGENHARIA DE TELECOMUNICAÇÕES

BRUNO SAMPAIO ROCHA

**ALGORITMO PARA DIMINUIÇÃO DA TAXA DE ERRO EM SISTEMAS DE
DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICAS USANDO PULSARES**

FORTALEZA

2024

BRUNO SAMPAIO ROCHA

ALGORITMO PARA DIMINUIÇÃO DA TAXA DE ERRO EM SISTEMAS DE
DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICAS USANDO PULSARES

Dissertação apresentada ao curso de Mestrado Acadêmico em Engenharia de Telecomunicações do PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELECOMUNICAÇÕES do *Campus* Fortaleza da Instituto Federal de Educação, Ciência e Tecnologia do Ceará, como requisito parcial à obtenção do título de mestre em Engenharia de Telecomunicações. Área de Concentração: Informação Quântica.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2024



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ
Av. 13 de maio, 2081 - Bairro Benfica - CEP 60040-531 - Fortaleza - CE - www.ifce.edu.br

AVALIAÇÃO

Processo: 23256.003128/2024-12

Interessado: Bruno Sampaio Rocha

BRUNO SAMPAIO ROCHA

ALGORITMO PARA DIMINUIÇÃO DA TAXA DE ERRO EM SISTEMAS DE DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICAS USANDO PULSARES

Dissertação apresentada ao curso de Pós-Graduação em Engenharia de Telecomunicações do Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE) - *Campus Fortaleza*, como requisito parcial para obtenção do Título de Mestre em Engenharia de Telecomunicações.
Área de concentração: Sistemas de Telecomunicações

Aprovado em: **20 / 03 / 2024**

BANCA EXAMINADORA

Documento assinado digitalmente
RUBENS VIANA RAMOS
Data: 10/04/2024 10:04:25-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. **Rubens Viana Ramos** - orientador
Universidade Federal do Ceará - UFC

Documento assinado digitalmente
FRANCISCO JOSE ALVES DE AQUINO
Data: 10/04/2024 15:58:25-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. **Francisco José Alves de Aquino**
Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

Documento assinado digitalmente
GUILHERME DE ALENCAR BARRETO
Data: 10/04/2024 10:48:19-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. **Guilherme de Alencar Barreto**
Universidade Federal do Ceará - DETI/UFC

Documento assinado digitalmente
VALDIVINO ALEXANDRE DE SANTIAGO JÚNIOR
Data: 10/04/2024 15:36:06-0300
Verifique em <https://validar.iti.gov.br>

Prof. Dr. **Valdivino Alexandre de Santiago Júnior**
Instituto Nacional de Pesquisas Espaciais - INPE

A Deus.

À minha família.

Aos mestres.

AGRADECIMENTOS

Agradeço a Deus, o autor e mantenedor da minha vida. Agradeço à minha família. Agradeço ao meu orientador Rubens Ramos e ao professor Fábio Alencar que me deram todo o suporte para a conclusão deste trabalho. Agradeço também o apoio dos colegas da turma. A todos que de alguma forma contribuíram para a realização deste trabalho, os meus sinceros agradecimentos.

"Nada há encoberto que não venha a ser revelado; e oculto que não venha a ser conhecido. Porque tudo o que disseses às escuras será ouvido em plena luz; e o que disseses aos ouvidos no interior da casa será proclamado dos eirados."
(Lucas 12:2-3.)

RESUMO

Neste trabalho estudou-se a viabilidade de uma distribuição de chaves criptográficas simétricas utilizando um pulsar como fonte de aleatoriedade. Além de outros requisitos tais como: disponibilidade técnica, radiotelescópios, equipamentos de leitura e transmissão de dados, se faz necessária a correção dos bits gerados pelas duas partes por meio da leitura dos dados de cada radiotelescópio, de forma que as duas partes da comunicação, aqui denominadas Alice e Bob, possam ter uma chave válida. Esta correção é necessária pois cada radiotelescópio utilizado para aquisição dos dados possui um ruído individual gaussiano intrínseco. Para tanto, neste trabalho se propõe a utilização de um algoritmo capaz de diminuir a taxa de erro dos bits gerados. No cerne do algoritmo proposto está a disentropia relativa, que, utilizando a função W_q de Lambert-Tsallis funciona como uma medida de distância entre distribuições de probabilidade e, quando aplicada à autocorrelação de cada sinal, funciona como medida de aleatoriedade. O algoritmo é descrito e o resultado das simulações é discutido.

Palavras-chave: Chaves Criptográficas. Pulsar. Disentropia. Função W_q de Lambert-Tsallis.

ABSTRACT

In this work, the feasibility of distributing symmetric cryptographic keys using a pulsar as a source of randomness was studied. In addition to other requirements such as technical availability, radio telescopes, data reading and transmission equipment, the correction of bits generated by both parties through the reading of data from each radio telescope is necessary so that both parties in communication, here referred to as Alice and Bob, can have a valid key. This correction is necessary because each radio telescope used for data acquisition has intrinsic individual Gaussian noise. To this end, this work proposes the use of an algorithm capable of reducing the error rate of the generated bits. At the heart of the proposed algorithm is relative disentropy, which, using the Lambert-Tsallis W_q function, serves as a measure of distance between probability distributions and, when applied to the autocorrelation of each signal, serves as a measure of randomness. The algorithm is described, and the results of the simulations are discussed.

Keywords: Cryptographic Keys. Pulsar. Disentropy. Lambert-Tsallis W_q Function.

LISTA DE FIGURAS

Figura 1 – Configuração de Transmissão do Sinal do Pulsar	13
Figura 2 – Cifra de César	18
Figura 3 – Frequência das letras no idioma português	19
Figura 4 – Scytale Espartano	20
Figura 5 – Geração de texto cifrado através da cifra de Vernam	23
Figura 6 – Exemplo de aplicação one-time pad	24
Figura 7 – Janela de pulsos do pulsar PSR B0301+19	27
Figura 8 – Geometria do Feixe de um Pulsar	29
Figura 9 – Interpulso em PSR B1702-19 (1,4GHz)	30
Figura 10 – Detecção de sinais de pulsares usando radiotelescópios	30
Figura 11 – $W_{2/3}(z)$ versus z	38
Figura 12 – $W_{4/5}(z)$ versus z	38
Figura 13 – Sinais com diferentes níveis de aleatoriedade	40
Figura 14 – Sinal de Alice antes da correção	45
Figura 15 – Sinal de Bob antes da correção	45
Figura 16 – Erro (antes e depois da correção)	46
Figura 17 – Chave de Alice corrigida	46
Figura 18 – Chave de Bob corrigida	47
Figura 19 – Sequência de 1000 pulsos de Alice (antes da correção)	47
Figura 20 – Sequência de 1000 pulsos de Alice (depois da correção)	48
Figura 21 – Sequência de 1000 pulsos de Bob (antes da correção)	48
Figura 22 – Sequência de 1000 pulsos de Bob (depois da correção)	48
Figura 23 – Aleatoriedade de Alice (antes e depois da correção)	49
Figura 24 – Aleatoriedade de Bob (antes e depois da correção)	49

LISTA DE TABELAS

Tabela 1 – Transposição colunar simples	20
Tabela 2 – Transposição por itinerário com duas linhas.	21
Tabela 3 – Disentropia de sinais periódicos e/ou aleatórios	40
Tabela 4 – BER média (antes e depois da correção)	49
Tabela 5 – BER (antes e depois da correção)	49
Tabela 6 – Aleatoriedade de Alice (antes e depois da correção)	50
Tabela 7 – Aleatoriedade de Bob (antes e depois da correção)	50

LISTA DE ABREVIATURAS E SIGLAS

BER	Bit Error Rate
eq.	equação
eqs.	equações
PVR	Publicly Verifiable Randomness
PDF	Probability Density Function
QKD	Quantum key Distribution
RFI	Radio Frequency Interference

SUMÁRIO

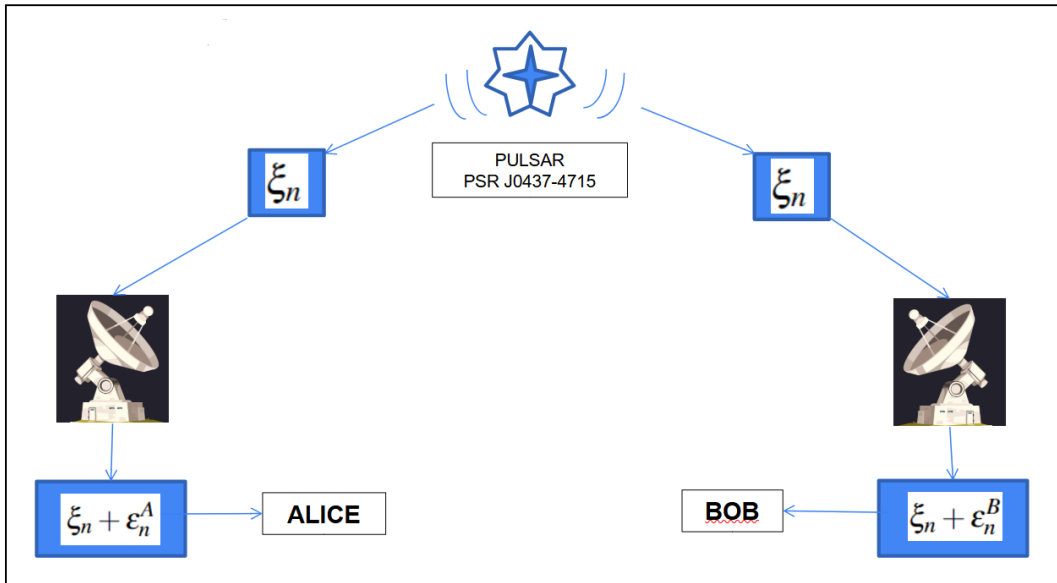
1	INTRODUÇÃO	12
1.1	Organização da Dissertação	13
2	CRIPTOGRAFIA	15
2.1	Contexto Geral	15
2.2	Contexto Histórico	18
2.3	Protocolos de Criptografia	22
3	PULSARES	26
3.1	Uma Visão Geral	26
3.2	Deteção de Sinais de Pulsares Usando Radiotelescópios	29
3.3	Utilização de Pulsares para Geração de Sinais Aleatórios	33
4	FUNÇÃO LAMBERT-TSALLIS (W_q)	36
4.1	Disentropia	38
5	SIMULAÇÃO NUMÉRICA DE UMA DISTRIBUIÇÃO DE CHAVES USANDO UM PULSAR	42
5.1	Parâmetros da Simulação	42
5.2	Aplicação do Algoritmo para Diminuição da Taxa de Erro	43
6	CONCLUSÃO E PERSPECTIVAS FUTURAS	51
6.1	Conclusão	51
6.2	Perspectivas Futuras	51
	REFERÊNCIAS	52
	APÊNDICE A – CÓDIGO DO ALGORITMO DE DIMINUIÇÃO DE TAXA DE ERRO (COMENTADO)	54

1 INTRODUÇÃO

A segurança da informação é uma preocupação presente na humanidade. Sempre houve a necessidade de se estabelecer comunicação em sigilo por diversos motivos: questões de segurança nacional, proteção financeira, privacidade, entre outros. Nesse contexto, a evolução da criptografia até hoje se mostra como uma maneira eficaz de garantir a privacidade de qualquer troca de informação. A criptografia simétrica requer que as partes legítimas interessadas na comunicação compartilhem uma chave comum para decodificar a mensagem. Esta chave, para ser válida, deve ser uma sequência de bits aleatória. Para compartilhar esta chave, é necessário um protocolo seguro de distribuição de chaves. As partes interessadas, denominadas neste trabalho de Alice e Bob, em geral, necessitam de uma terceira parte confiável para realizar esta distribuição de forma segura. De acordo com Lo, Curty e Tamaki (2014), Scarani *et al.* (2009) e Fröhlich *et al.* (2015), até o presente momento, protocolos de distribuição de chaves quânticas (*quantum key distribution (QKD)*) são reconhecidamente os protocolos de distribuição de chaves criptográficas com o maior nível de segurança, contudo, os protocolos QKD utilizam fótons individuais ou estados coerentes fortemente atenuados, o que limita a distância de comunicação entre Alice e Bob a algumas centenas de quilômetros devido às perdas na conexão óptica (CHEN *et al.*, 2021). Esforços para superar esta limitação de distância estão em andamento por meio da utilização de repetidores quânticos, porém, estes ainda não estão disponíveis para uso. Sendo assim, uma proposta interessante de protocolo de distribuição de chaves foi apresentada por Dawson (2022) e outros, que utiliza a dinâmica de pulsos de uma estrela pulsar para geração dos números aleatórios necessários. Para tanto, dois radiotelescópios, um na Austrália e outro na China, cuja distância entre eles está na ordem de milhares de quilômetros, recebem sinais (pulsos eletromagnéticos) simultaneamente do mesmo pulsar (PSR J0437-4715) e utilizam a aleatoriedade da densidade de fluxo medida para criar uma sequência aleatória de bits comum entre os dois (Figura 1). Foram utilizados três métodos para extrair bits dos valores de densidade de fluxo. No primeiro método, que utiliza a mediana dos valores medidos, cada pulso proveniente do pulsar produz um bit da chave. Nos outros dois métodos, um bloco de pulsos é usado para produzir um bit da chave, o que reduz a taxa de erro de bits (BER) em detrimento da taxa de transmissão dos bits. Após as medições da densidade de fluxo e extração dos bits, Alice e Bob precisam executar protocolos de correção de erros e amplificação de privacidade para obter uma chave final segura e útil (LO; CURTY; TAMAKI, 2014), (SCARANI *et al.*, 2009) e (FRÖHLICH *et al.*, 2015). Estes protocolos de correção de erros e amplificação de privacidade reduzem o

comprimento da chave, e o número de bits perdidos depende da taxa de erro de bits (*bit error rate* (BER)). Quanto maior a BER, maior o número de bits perdidos. A BER máxima permitida é de 11%, quando a fração de bits da chave perdidos durante o procedimento de correção de erros tende a 100%. Estes erros ocorrem principalmente devido ao ruído intrínseco (gaussiano) dos radiotelescópios e, portanto, são inevitáveis. Nesse trabalho, portanto, apresenta-se um algoritmo que reduz a taxa de erro da chave comum, permitindo que Alice e Bob usem o método mais simples de extração de bits e obtenham um bit por pulso proveniente do pulsar. No cerne do algoritmo proposto está a disentanglement como medida da distância entre distribuições de probabilidade e, por extensão, de aleatoriedade. A disentanglement, por sua vez, utiliza a função W_q de Lambert-Tsallis para sua aplicação (SILVA; RAMOS, 2019) .

Figura 1 – Configuração de Transmissão do Sinal do Pulsar



Fonte: o autor.

1.1 Organização da Dissertação

Capítulo 2: Neste capítulo é delineado um contexto histórico sobre criptografia, abordando algumas técnicas e conceitos atuais.

Capítulo 3: Neste capítulo é introduzido o conceito de pulsar, são mostradas as técnicas de aquisição de dados destes pulsares a partir de radiotelescópios e como estes dados podem ser utilizados para geração de sequências aleatórias.

Capítulo 4: Neste capítulo é feita uma revisão da função W_q de Lambert-Tsallis e da disentanglement como medida de distância entre distribuições de probabilidade, bem como para medição de

aleatoriedade dos dados trabalhados nesta pesquisa.

Capítulo 5: Finalmente, neste capítulo tratam-se os dados utilizados na simulação de sequências aleatórias. O algoritmo de correção de erros proposto é apresentado e simulações numéricas são realizadas demonstrando a eficácia deste método de diminuição de erros e, consequentemente, de validação das chaves criptográficas.

2 CRIPTOGRAFIA

2.1 Contexto Geral

A palavra criptografia é derivada das raízes gregas: *kryptos* (secreto) e *graphia* (mensagem). De acordo com Costa (2010), técnicas para ocultar mensagens e/ou transmiti-las de modo secreto já são utilizadas há muitos anos. Sacerdotes egípcios utilizavam hieróglifos, que eram incompreensíveis para a maior parte da população que utilizava a língua demótica (COSTA, 2010). Da mesma forma, os babilônios utilizavam a escrita cuneiforme. Segundo o historiador grego Heródoto, um grego que precisava transmitir uma mensagem de forma secreta tatuava a mensagem que desejava ocultar na cabeça raspada, esperava o cabelo crescer e posteriormente raspava novamente a cabeça ao chegar ao destinatário, de forma a revelar a mensagem. Em outro caso, mensagens foram escritas em madeiras e posteriormente foram cobertas com cera, de forma a transmitir uma mensagem para a Grécia acerca de preparativos de uma invasão organizada pelo rei persa Xerxes. Desta forma, os gregos puderam se preparar adequadamente para o embate, derrotando assim a frota invasora. Estas técnicas rudimentares citadas anteriormente são chamadas de "esteganografia". Neste caso, apenas ocultam a mensagem, porém, caso o inimigo consiga interceptar a mensagem esta já se encontra decodificada, de modo que não se necessita nenhum esforço adicional para desvendar o conteúdo (COSTA, 2010).

A criptografia, de outra forma, é uma técnica em que a mensagem não é compreensível por outra pessoa que não seja o destinatário. Para que esta comunicação secreta aconteça, a mensagem deve ser embaralhada (codificada) de tal maneira que apenas o emissor e o receptor conheçam uma maneira (chave) de reorganizar (decodificar) a mensagem de forma a torná-la legível novamente. Portanto, a criptografia não se trata primariamente de ocultar a mensagem, e sim de torná-la decifrável somente para o destinatário. As técnicas de esteganografia e criptografia podem ser utilizadas de forma conjunta, aumentando o nível de segurança (COSTA, 2010).

A criptografia, bem como outras técnicas de segurança da informação, são utilizadas como resposta a diversos tipos de ataques. Pode-se definir um ataque a um sistema de informação como uma busca de acesso não autorizado às informações pertinentes a ele. Existem diversos tipos de ataques e trapças que podem comprometer a segurança e o sigilo de mensagens e dados transmitidos:

- a) **violação de privacidade:** acontece quando o invasor consegue acessar a

informação ou conteúdo da mensagem sem autorização das partes envolvidas na comunicação;

- b) **falsificação de identidade:** ocorre quando alguém usa de diversos meios para se passar por outra pessoa, fazendo com que a outra parte da comunicação acredite estar se comunicando com o interlocutor que teve a identidade falsificada;
- c) **negação de responsabilidade:** acontece quando alguém cria/envia uma informação e, posteriormente, por diversos motivos, nega que o fez;
- d) **negação de recebimento de informação:** esse tipo de fraude ocorre quando alguém nega ter recebido uma mensagem;
- e) **falsificação de informação recebida:** ocorre quando o fraudador recebe de uma pessoa uma mensagem, porém divulga uma mensagem diferente para terceiros como sendo aquela recebida originalmente;
- f) **troca ou interrupção de informação:** este tipo de fraude acontece quando um atacante intercepta uma mensagem entre duas pessoas, modificando-a, sem que isto seja detectado pelas duas partes (emissor e receptor) ou mesmo quando impede que esta informação seja disponibilizada para o receptor (COSTA, 2010).

Estes são apenas alguns exemplos de ataques que podem ocorrer em um sistema de comunicação. Estes ataques ainda podem ser classificados em ativos e passivos, quando há e quando não há, respectivamente, a manipulação da mensagem transmitida, ou seja, ataques passivos, como por exemplo, (interceptar o conteúdo de uma mensagem sem alterá-la), em geral, são mais difíceis de serem detectados. Muitos invasores podem utilizar outros meios de fraudar uma comunicação ou mesmo mesclar diversas modalidades em um mesmo ataque. Dadas as ameaças potenciais que um sistema de troca de informações pode sofrer, os sistemas criptográficos devem oferecer serviços que possam garantir a total confiabilidade nesse sistema de informação. Essa confiabilidade deve se dar em diversos níveis e aspectos da comunicação de forma que esta possa ser realizada de maneira plenamente segura e sigilosa. Em geral, um modelo de segurança prevê a atuação de um possível atacante e uma terceira parte confiável, além das duas (ou mais) partes principais interessadas na comunicação. O atacante, como o próprio nome sugere, é a figura que tentará de diversas formas quebrar a segurança da informação. Por outro lado, esta terceira parte confiável geralmente é a entidade que intermediará a comunicação,

seja distribuindo chaves entre as partes ou mesmo garantindo a autenticidade de assinaturas digitais. Conforme explica Costa (2010), os serviços e garantias que devem ser oferecidos por protocolos de segurança e sistemas criptográficos são:

- a) **confidencialidade ou sigilo:** este é um dos aspectos mais importantes da proteção da informação. A confidencialidade garante a proteção da mensagem contra ataques passivos. Esta proteção pode ser feita fisicamente ou por meio de protocolos para torná-la ininteligível a agentes não autorizados. Outro aspecto importante do sigilo em uma troca de informações é a proteção contra análise de tráfego. Um invasor não necessariamente precisa conhecer o conteúdo de uma informação enviada para extrair dados importantes desta: a origem, destino, tamanho, frequência e outros aspectos de um tráfego de informação podem ser extremamente relevantes dependendo do contexto. Durante uma guerra, os inimigos podem descobrir a localização da origem ou destino de determinadas mensagens (através de triangulação de sinais de rádio, por exemplo) e direcionar seus ataques para estes locais;
- b) **autenticidade:** autenticar uma mensagem tem o objetivo de garantir que as partes da comunicação estejam efetivamente se comunicando com as respectivas partes desejadas. Em uma comunicação bidirecional entre duas partes (Alice e Bob), por exemplo, uma comunicação autêntica deve garantir a Alice e Bob que estes estejam recebendo e enviando mensagens para ambos de fato, e não para um invasor tentando se passar por um dos dois (ou pelos dois). Para garantir a autenticidade, em geral, o sistema deve pedir determinadas credenciais que só podem ser apresentadas ou conhecidas por um ente legítimo da comunicação, tais como: senhas, cartões, impressão digital, traços faciais, dentre outros. Atualmente uma maneira de garantir a autenticidade das comunicações são as assinaturas digitais;
- c) **integridade:** é a garantia de que o conteúdo de uma mensagem não foi alterado. O conteúdo pode ser alterado de maneira acidental ou proposital;
- d) **não-repúdio:** este aspecto da segurança garante que o emissor ou o receptor da mensagem não possam negar que tenham recebido ou emitido uma informação que efetivamente o tenham feito. Isto está intimamente relacionada com a autenticidade da comunicação;

- e) **controle de acesso:** o controle de acesso restringe o acesso de determinadas informações e/ou sistemas a um ente ou grupo específico. Esta é outra característica que está relacionada diretamente com a autenticidade, já que os mecanismos de restrição se dão através de autenticação de usuários;
- f) **disponibilidade:** a disponibilidade da informação é um aspecto crucial em uma troca de informações. Muitos ataques maliciosos se concentram somente em atacar a disponibilidade. Em uma guerra, é muito comum que os inimigos tentem impedir a plena comunicação da outra parte do conflito, ou mesmo criminosos podem sobrecarregar um servidor de web de forma a tirar algum sítio ou sistema do ar.

2.2 Contexto Histórico

De acordo com Zochio (2016), uma das primeiras cifras de que se tem conhecimento no ocidente é a **cifra de César**, que consiste em uma substituição monoalfabética. Neste tipo de codificação, cada letra é substituída por outra a x posições de distância na distribuição alfabética. O número x , portanto, é a chave para decodificar a mensagem. A cifra de César segue portanto a seguinte lógica:

-Cifrar: $C = O + x$;

-Decifrar: $O = (C - x)$;

onde: C = cada letra do texto cifrado; x = deslocamento escolhido; O = cada letra do texto original.

Como se pode observar, no alfabeto do idioma português, o número máximo de deslocamentos é $x = 25$. Um exemplo de cifragem com deslocamento $x = 3$ é: **Palavra original** "Disentropia"; **Palavra cifrada** "Gmvhqxurmd".

A cifra de César (Figura 2), assim como outras cifras de substituição primitivas podem ser decifradas através do método da "força-bruta", que consiste basicamente na tentativa de inserir cada uma das chaves possíveis até obter êxito, já que no caso desta, o número de tentativas é menor ou igual a 25. A chave original utilizada pelo imperador César previa 3 deslocamentos de texto.

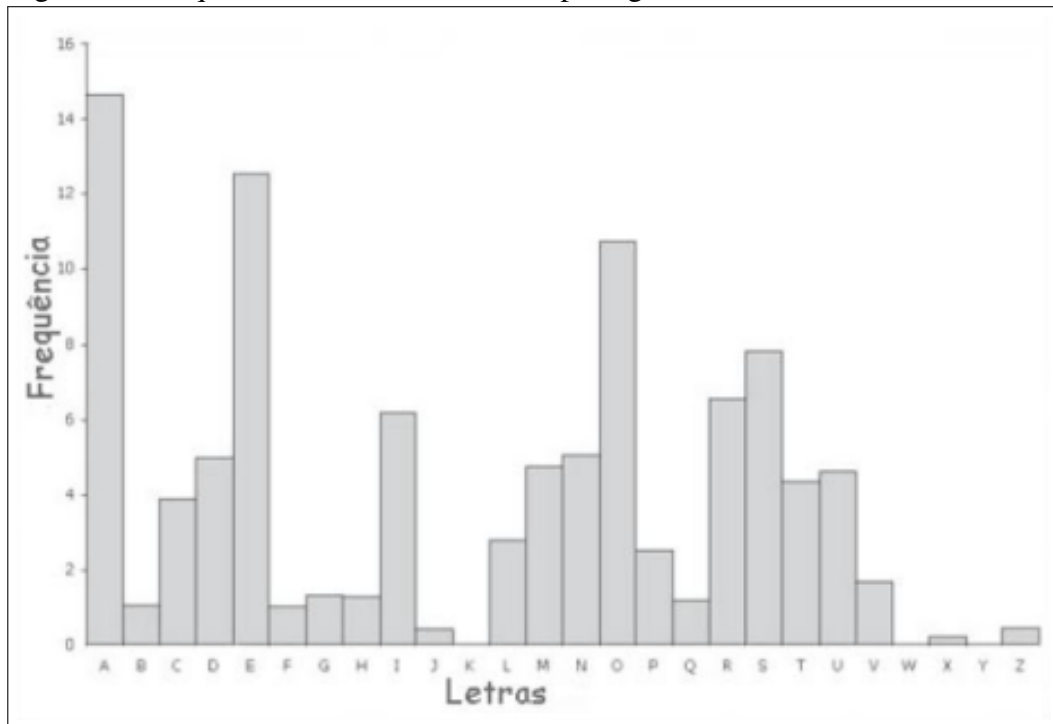
Figura 2 – Cifra de César

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: o autor.

Outra análise que deve ser levada em conta é a de que, em cada alfabeto, existe uma distribuição característica de frequência das letras em textos gerais. Por exemplo, na língua portuguesa, em geral a letra A, seguida das letras E, O, S, R, I, D, N, M e U constituem as dez letras mais utilizadas em textos de forma geral, conforme mostra a Figura 3.

Figura 3 – Frequência das letras no idioma português



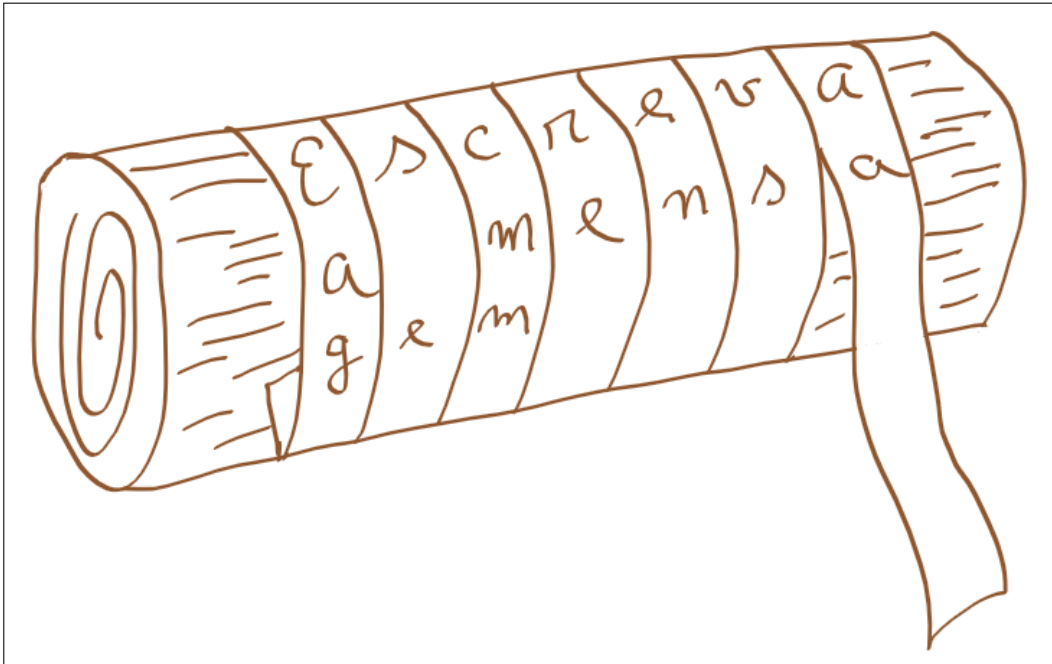
Fonte: (ZOCHIO, 2016).

Desta forma, mesmo que a substituição das palavras não tenha um único deslocamento ao longo do texto, ou mesmo que cada caractere seja substituído por outro arbitrariamente sem seguir uma sequência de deslocamento alfabético, uma análise do texto baseada na frequência com que os caracteres aparecem pode mostrar um excelente ponto de partida para a descoberta da mensagem original. Portanto, quanto maior o texto, mais fácil será para um analista descobrir a chave da cifra utilizada (ZOCHIO, 2016). A análise realizada para decodificar uma cifra é chamada: **criptoanálise**.

Neste contexto, pode-se mencionar também a transposição, que consiste em uma técnica criptográfica tão antiga quanto a técnica de substituição. Segundo Zochio (2016), cifras que se baseiam em transposição trocam as posições dos caracteres do texto plano seguindo um padrão. Um exemplo notável dessa técnica descrita por Plutarco em 90 d.C, é o "Scytale Espartano"(Figura 4). Este instrumento consistia em um bastão de madeira, no qual era enrolada uma fita onde se escrevia a mensagem desejada em colunas verticais ao longo do bastão. Após a fita ser desenrolada, a mensagem ao longo da fita estava indecifrável. Para decifrá-la novamente

era necessário enrolar novamente a fita em um bastão de mesmo comprimento e diâmetro daquele no qual a mensagem foi escrita. Dito isto, percebe-se claramente alguns elementos fundamentais da criptografia no scytale: o bastão funciona como a chave criptográfica e os atos de enrolar e desenrolar são análogos a cifrar e decifrar a mensagem, respectivamente (COSTA, 2010).

Figura 4 – Scytale Espartano



Fonte: o autor.

Alguns exemplos de transposições geométricas são:

- a) **transposição colunar simples**: O texto é inserido em uma matriz/tabela, no sentido das linhas e a saída do texto criptografado consiste em transcrever o texto lido no sentido das colunas. Na Tabela 1 pode-se ver a aplicação no texto "Penso, logo existo", que cifrado ficaria "PLXEOINGSSOTOEO";

Tabela 1 – Transposição colunar simples

P	E	N	S	O
L	O	G	O	E
X	I	S	T	O

Fonte: (ZOCHIO, 2016).

- b) **transposição linear simples**: funciona da mesma forma que a transposição colunar, porém as colunas são substituídas por linhas e vice-versa;

- c) **transposição por itinerário:** neste modelo usa-se um itinerário para definir as figuras geométricas utilizadas na cifra. Este tipo de codificação foi utilizado na Guerra Civil norte-americana (1861-1865). Na Tabela 2 tem-se o mesmo texto utilizado na Tabela 1.

Tabela 2 – Transposição por itinerário com duas linhas.

P		N		O		O		O		X		S		O
	E		S		L		G		E		I		T	

Fonte: (ZUCHIO, 2016)

Existem infinitas possibilidades de transposição: espirais, em L, com chaves numéricas, dentre outras. Todas utilizando o mesmo princípio (ZUCHIO, 2016).

Como visto anteriormente, a análise de frequências explora uma debilidade intrínseca às cifras monoalfabéticas. Quanto maior o texto, maior é a probabilidade deste apresentar uma distribuição de frequências característica de cada idioma (Figura 3). Este tipo de estudo, cujo primeiro registro se dá no livro "Escritos sobre a decifração de mensagens criptográficas", escrito pelo árabe al-Kindy, formalizou cientificamente a criptoanálise (COSTA, 2010). Por volta do século XIV, a Itália foi um dos primeiros países a encarar a criptografia de forma sistemática, criando para isso um órgão governamental dedicado ao estudo da criptografia. A idade moderna, identificada pelo início do movimento Renascentista, iniciou por volta de 1450 e durou até o final século XIX. Neste período, houve avanços significativos em todas as áreas do conhecimento humano, com destaque à arte e às ciências (COSTA, 2010). De acordo com Zuchio (2016) Blaise de Vigenère (1523-1596) criou, em 1580, a famosa cifra que leva seu nome. A inovação da cifra de Vigenère se dá pelo uso da substituição polialfabética acrescida do uso de uma chave. À época, esta codificação era bastante sofisticada, e seu reinado durou quase 300 anos. O matemático inglês Charles Babbage (1791-1871) conseguiu quebrar esta cifra em 1854, porém este fato ficou anônimo por bastante tempo e oficialmente a superação da cifra de Vigenère é creditada ao criptógrafo alemão Friedrich Kasiski (1805-1881) em 1863 (COSTA, 2010). Desde então, diversas outras técnicas foram desenvolvidas. A teoria dos números e o estudo dos números primos fundamentaram um grande avanço nas técnicas criptográficas. Atualmente, os protocolos de distribuição de chaves quânticas (QKD) se mostram como os meios mais seguros de garantir a segurança da transmissão destas chaves (LO; CURTY; TAMAKI, 2014; SCARANI *et al.*, 2009; FRÖHLICH *et al.*, 2015).

2.3 Protocolos de Criptografia

Phil Zimmermann, um engenheiro de software americano nascido em 1954 criou o PGP (Pretty Good Privacy), um programa de segurança para correio eletrônico disponível de forma livre (COSTA, 2010). O PGP utiliza uma combinação de um protocolo de chave privada chamado IDEA e um protocolo de chave pública (RSA), que é utilizado para a troca da chave que será usada no IDEA. O PGP é usado para criptografar e descriptografar e-mails e arquivos confidenciais. O PGP é bastante popular devido à facilidade de uso e à confiança como um dos softwares de criptografia mais seguros disponíveis (COSTA, 2010). Como dito anteriormente, a criptografia de chave pública é um método de criptografia que utiliza duas chaves diferentes para criptografar e descriptografar dados. A chave pública é distribuída publicamente e é usada para criptografar os dados, já a chave privada deve ser mantida em segredo pois é utilizada para decifrar os dados. No coração do protocolo RSA está a incapacidade (com os meios tecnológicos atuais) de se fatorar números primos muito grandes. Neste caso, o protocolo utiliza dois números primos grandes para criar as chaves pública e privada. A chave pública, como é amplamente conhecida, utiliza o produto desses dois números primos, enquanto a chave privada é composta pelos números primos fatores deste produto (SOUSA, 2013). O início do esquema RSA se deu em 1976, quando Whitfield Diffie e Martin Hellman publicaram o livro "*New Directions in Cryptography*". Esse texto respondia ao problema de se trocar mensagens inicialmente em um sistema aberto, porém, sendo necessário que ao final do processo a chave fosse conhecida apenas pelos interlocutores autênticos (COSTA, 2010). A função usada por Diffie e Hellman sugeria a utilização de uma combinação de função exponencial com aritmética modular, sendo denominada no jargão da criptografia como função de mão única. Neste ponto, a implementação desta solução era puramente teórica (COSTA, 2010). De acordo com Stallings (2014), este problema se tornou um desafio para os criptologistas, e de certa forma, lançou as bases para o conceito de chave pública. Diversos algoritmos falharam, porém uma das primeiras respostas concretas para o problema foi desenvolvida em 1977, por Ron Rivest, Adi Shamir e Len Adleman, no MIT, e publicada em 1978 (STALLINGS, 2014). O esquema que leva as iniciais dos nomes Rivest-Shamir-Adleman (RSA), desde então, tem se mostrado como a principal técnica para a encriptação de chave pública (STALLINGS, 2014). A chave privada (usada para decifrar a mensagem) consiste de dois números primos p e q muito grandes, enquanto a chave pública (usada para cifrar a mensagem) é definida por n , onde $n = p \times q$. Esta chave pode ser comunicada publicamente. Mais detalhes do esquema RSA podem ser encontrados em (STALLINGS, 2014;

SOUSA, 2013; COSTA, 2010).

De acordo com Stallings (2014), a cifra de Vernam é uma técnica de criptografia criada por um engenheiro da AT&T Gilbert Vernam em 1918. Esse sistema funciona sobre dados binários, ao invés de letras, portanto a mensagem original é combinada bit a bit com a chave, usando uma operação lógica XOR (ou exclusivo) para produzir uma mensagem cifrada. A mensagem cifrada pode então ser decifrada de forma semelhante, combinando-a com a mesma chave original usando a operação XOR, decifrando a mensagem original. Esse sistema pode ser descrito conforme a eq. 2.1 e seus esquema de transmissão é mostrado na Figura 5.

$$c_i = p_i \oplus k_i \quad (2.1)$$

onde:

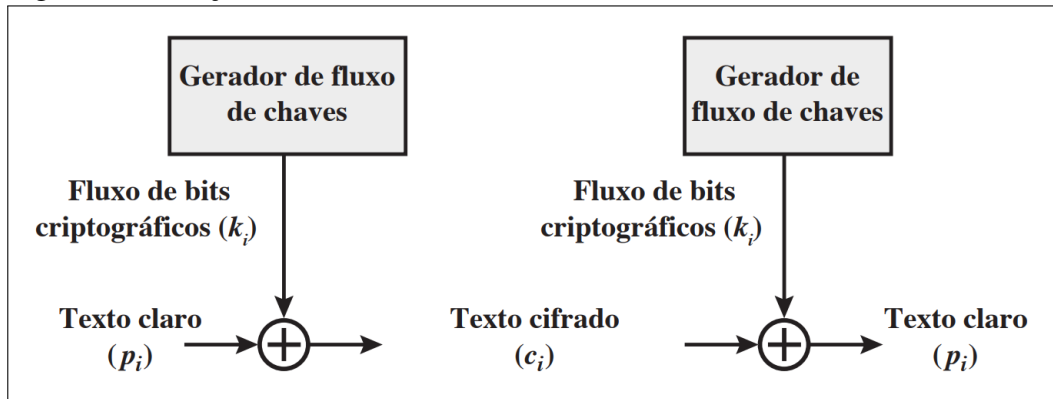
(p_i) é o dígito binário na posição (i) do texto claro;

(k_i) é o dígito binário na posição (i) da chave;

(c_i) é o dígito binário na posição (i) do texto cifrado;

$(\oplus)$ representa a operação ou-exclusivo (XOR).

Figura 5 – Geração de texto cifrado através da cifra de Vernam



Fonte: (STALLINGS, 2014).

Assim, devido às propriedades da operação XOR (ou-exclusivo) para a decriptação da mensagem, basta apenas que se use a mesma operação bit a bit, conforme descrito na eq.2.2.

$$P_t = c_t \oplus k_t \quad (2.2)$$

A cifra de Vernam é considerada uma das técnicas mais seguras de criptografia devido à sua simplicidade e à sua propriedade de proporcionar perfeito sigilo, desde que a chave seja

verdadeiramente aleatória, secreta e usada apenas uma vez. A dificuldade na implementação da cifra de Vernam está no fato de que deve ser gerada uma chave aleatória secreta a cada transmissão de mensagem. Para tanto, o protocolo de distribuição destas chaves deve garantir o seu sigilo. Outra desvantagem relevante da cifra de Vernam é que esta não fornece garantia de autenticação no envio das mensagens. A essência da técnica é o modo como a chave é construída. Vernam estabeleceu uma palavra-chave muito longa, porém que eventualmente era repetida. Embora uma criptoanálise de uma chave longa seja difícil de ser implementada, uma fragilidade desse tipo de técnica é que ela pode ser quebrada usando um número suficiente de texto cifrado com a utilização de sequências de textos decifrados conhecidos e/ou prováveis.

Segundo Stallings (2014), Joseph Mauborgne, um oficial do Exército estadunidense, propôs uma melhoria na cifra de Vernam de forma a torná-la tão segura quanto possível. Ele sugeriu a utilização de uma chave tão grande quanto a mensagem a ser transmitida, de forma que a chave não precisasse ser repetida. Esta cifra utiliza uma chave de criptografia única e aleatória, de mesmo tamanho da mensagem a ser codificada e não possuindo nenhuma relação estatística com esta. Essa chave é usada apenas uma vez e depois deve ser descartada. Seu nome "*one-time pad*" se deve a este fato. Cada nova mensagem exige uma nova chave de mesmo tamanho. Como essa técnica produz uma saída aleatória e não existe nenhuma relação estatística com o texto original, ela é considerada inquebrável. Na Figura 6 tem-se um exemplo de aplicação do esquema *one-time pad*. Considera-se o texto cifrado "ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS". Tem-se neste exemplo duas decifrações distintas usando duas chaves diferentes. Mesmo que um criptoanalista conseguisse encontrar as duas chaves, dois textos claros plausíveis são encontrados. Qualquer desses textos poderia ser o texto original, desta forma, impedindo que se conheça a chave correta.

Figura 6 – Exemplo de aplicação one-time pad

texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	<i>pxlmvmsydofoyrvzwc tnlebnecvgdupahfzzlmnyih</i>
texto claro:*	mr mustard with the candlestick in the hall
texto cifrado:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
chave:	<i>mfugpmydgaxgoufhklllmhsqdgogtewbqfggyovuhwt</i>
texto claro:**	miss scarlet with the knife in the library

Fonte: (STALLINGS, 2014).

Apesar de sua utilidade limitada, a cifra de Vernam continua sendo uma técnica de criptografia relevante, principalmente para canais de pouca largura de banda que exigem alto nível

de segurança. Mesmo com as dificuldades de proteção e distribuição das chaves, o *one-time pad* é o único criptosistema que apresenta o que é conhecido como "segredo perfeito" (STALLINGS, 2014).

3 PULSARES

3.1 Uma Visão Geral

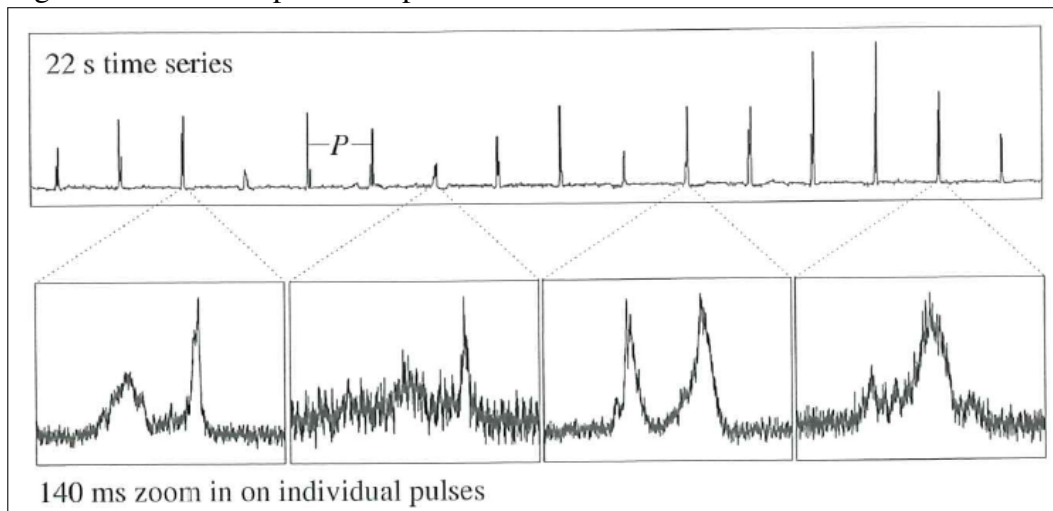
De acordo com Lyne e Graham-Smith (2012), dois astrônomos, Walter Baade e Fritz Zwicky, propuseram em 1934 a existência de uma nova forma de estrela, até então desconhecida: a estrela de nêutrons, que poderia ser o estágio final da evolução estelar. As condições extremas presentes em uma estrela de nêutrons estão além daquelas experimentadas cotidianamente em laboratórios. A densidade dessas estrelas está na ordem de $10^{14} g/cm^3$ e campos magnéticos na ordem de $10^{15} Gauss$ ($10^{11} Tesla$). Estas condições são encontradas em estrelas com aproximadamente 1,4 massas solares, porém compactadas em um raio de cerca de 10km (LYNE; GRAHAM-SMITH, 2012). Pacini, em 1967, propôs que a fonte de energia da nebulosa do Caranguejo deveria ser a rápida rotação de uma estrela de nêutrons altamente magnetizada (LYNE; GRAHAM-SMITH, 2012). Pulsares são estrelas de nêutrons altamente magnetizadas em rápida rotação. Estas estrelas produzem feixes eletromagnéticos de rádio e outras faixas de frequência no universo como faróis. Foram descobertos por Jocelyn Bell-Burnell e Anthony Hewish em 1967 e desde então outros milhares já foram descobertos. Muitos desses pulsares foram descobertos através do telescópio Parkes. Este radiotelescópio de 64m de diâmetro é capaz de coletar dados de treze pontos do céu independentes de forma simultânea (LYNE; GRAHAM-SMITH, 2012).

A astronomia de pulsares é um campo de estudos que envolve uma grande faixa de comprimentos de onda e também é responsável pelos primeiros estudos experimentais de ondas gravitacionais (LORIMER; KRAMER, 2004). Um pulsar de milissegundos (*MSP-millisecond pulsar*) é assim chamado devido ao seu período de rotação, que é da ordem de milissegundos (*ms*). O (MSP) PSR J0437-4715 foi descoberto em 1993 e é um dos pulsares mais brilhantes (densidade de fluxo espectral $S_{1400} = 150,2 mJy$) e mais próximos ($d = 156,79 \pm 0,25 pc$) pulsares conhecidos. Ele tem um período curto de $P = 5,758 ms$ e se destaca por ter uma taxa de rotação extremamente estável, tornando-o um relógio natural com estabilidade semelhante à de um relógio atômico. Ele faz parte de um sistema binário com órbita circular de 5,74 dias de período, onde a estrela secundária é uma anã branca de aproximadamente 0,2 massas solares (FISCELLA *et al.*, 2021).

Uma das propriedades mais evidentes e interessantes dos pulsares é o "Efeito Farol". Este efeito pode ser facilmente caracterizado como uma função de pulsos no tempo. Os pulsos

individuais variam muito de um para o outro, e um único pulso de um pulsar pode se manifestar apenas como um dos componentes do perfil integrado. Esses sub-pulsos oferecem pouca indicação da forma característica do perfil integrado, no entanto, devido à periodicidade precisa dos pulsares, é possível construir um perfil de pulso integrado a partir de algumas centenas ou milhares de pulsos individuais (LYNE; GRAHAM-SMITH, 2012). Por exemplo, conforme mostra a Figura 7, o pulsar PSR B0301+19 demonstra uma regularidade de pulsos com um período de repetição de $P = 1,38s$ em uma janela de $22s$ e concomitantemente uma ampliação de $140ms$ mostra mais detalhes destes pulsos. Atualmente sabe-se que esses pulsos regulares são emitidos a cada vez que o feixe de emissão (farol) está apontado para o instrumento de detecção. Desta forma se pode calcular precisamente a frequência de rotação, que no exemplo do pulsar PSR B0301+19 é de $f = (1/P) = 0,725Hz$ (LORIMER; KRAMER, 2004).

Figura 7 – Janela de pulsos do pulsar PSR B0301+19



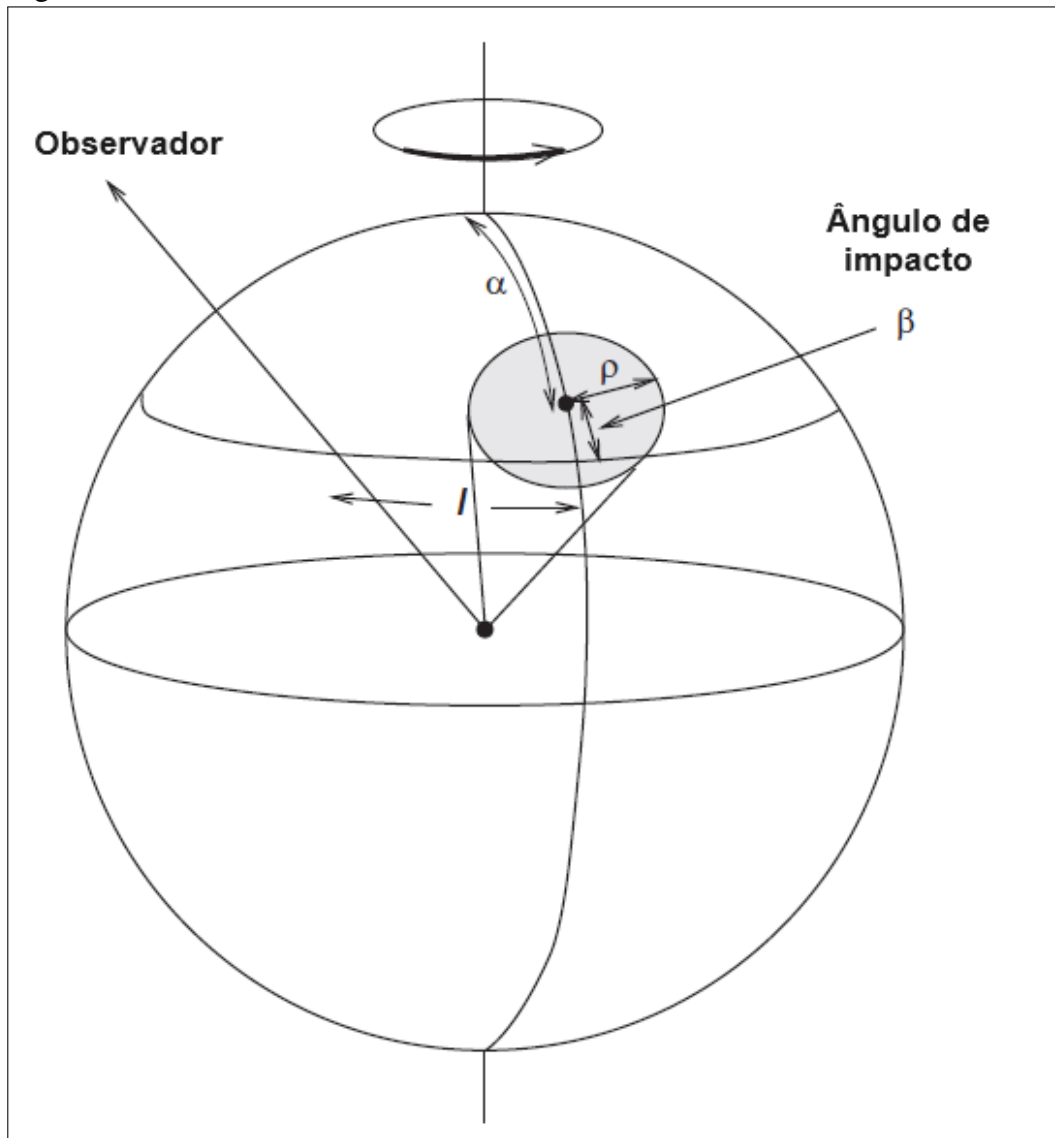
Fonte: (LORIMER; KRAMER, 2004).

De acordo com Lyne e Graham-Smith (2012), os pulsares radiam pulsos de perfis únicos, diferindo de pulsar para pulsar. O surgimento do telescópio via satélite Fermi LAT e os detectores do tipo "*air shower Cerenkov*" HESS e VERITAS abriram uma nova perspectiva para observar a radiação direcionada de alta energia dos pulsares e das nebulosas de vento, que têm suas dinâmicas definidas pelos ventos causadas pelos feixes dos pulsares. Muitos pulsares de milissegundos e pulsares jovens, especialmente aqueles com grande energia de desaceleração, são observáveis com o LAT. Vale destacar que nos regimes de alta energia, a radiação é detectada como fótons individuais, de forma que para se enxergar o formato do pulso é necessária uma integração da observação de milhões de emissões desses fótons. Embora os pulsos sejam emitidos em diversas faixas do espectro eletromagnético (incluindo raios gamma altamente energéticos),

a maioria dos pulsares é observável apenas em frequências de rádio, que é o caso específico deste trabalho. A geometria dos feixes emitidos por um pulsar pode ser vista na Figura 8, onde o feixe é mostrado com largura angular 2ρ a um ângulo de inclinação α em relação ao eixo de rotação. A linha de visão corta o feixe em um ângulo de impacto β em relação ao centro do cone. Frequentemente se assume que o cone de emissão tem simetria circular, porém há sugestões de que pode haver distorções e alongamentos no sentido latitudinal ou longitudinal. Através das características de polarização, podemos inferir informações sobre o parâmetro de impacto, mesmo quando α não é diretamente conhecido. O ângulo de inclinação α , geralmente, é mais difícil de determinar. Quando não se sabe determinar α com precisão, é frequentemente útil assumir que $\alpha = 90^\circ$. Esses valores calculados de ρ_{90} então superestimarão a largura real do feixe quando α é pequeno, de modo que as distribuições de ρ_{90} para vários pulsares terão um limite inferior relacionado a uma largura média real do feixe. Independentemente do método de oscilação de polarização, as larguras observadas dos componentes dentro do perfil podem ser usadas para determinar o ângulo de inclinação α . Esta possibilidade surge porque os feixes individuais dos componentes parecem ser aproximadamente simetricamente circulares, de modo que as larguras dos componentes não dependem da maneira como são cortados pela linha de visão. Além disso, suas larguras, determinadas para pulsares de um período dado e em uma frequência específica, são encontradas com uma distribuição bastante estreita.

Nas regiões laterais do perfil principal do pulso, a densidade de fluxo cai abruptamente, porém alguns pulsares apresentam um **interpulso** aproximadamente na metade do ciclo (180°) conforme mostra a Figura 9. A interpretação deste fenômeno é muitas vezes de que se trata de um feixe de radiação em direção oposta, que ocorre quando o ângulo α (Figura 8) entre o eixo do dipolo magnético do pulsar e o eixo de rotação é aproximadamente 90° . Isto também é um indício de que se trata de um pulsar jovem. O perfil do pulso detectado depende da relação entre a linha de visão do observador e o feixe de radiação que está contido em um cone alinhado a um pólo magnético (Figura 8), portanto a observação do interpulso sugere que a linha de visão está alinhada com o eixo magnético do pulsar. Além disso, a distribuição de fluxo dentro do feixe não é assimétrica. Convencionalmente, a largura total do perfil é medida em um nível arbitrário de 10% (W_{10}) da intensidade de pico. Como dito anteriormente, a queda é muito rápida fora do perfil principal. Alguns perfis medidos de pulsares estão na faixa entre 0,1 a 32GHz e a largura dos perfis de pulso é bem independente da frequência para frequências de rádio acima de 1GHz. Para frequências menores há uma expansão destes perfis (LYNE; GRAHAM-SMITH, 2012).

Figura 8 – Geometria do Feixe de um Pulsar

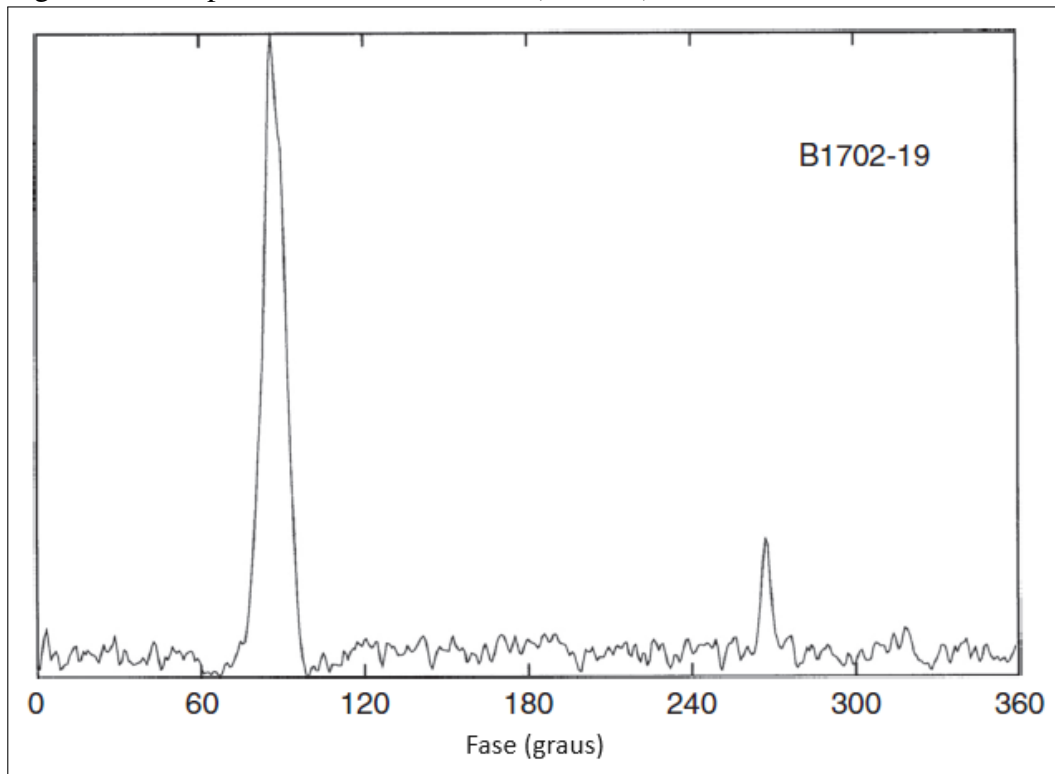


Fonte: Adaptado de (LYNE; GRAHAM-SMITH, 2012)

3.2 Detecção de Sinais de Pulsares Usando Radiotelescópios

Como objetos astronômicos estão muito distantes, as observações destes sempre consideram que as frentes de onda recebidas são paralelas. Um radiotelescópio é um dispositivo usado para amostrar o plano do campo elétrico dessa radiação, que, em geral, é uma grandeza vetorial variável no tempo. As antenas dos radiotelescópios coletam e concentram as ondas planas do sinal de entrada de forma que a radiação chegue ao alimentador de forma coerente, em fase e com as amplitudes somadas (Figura 10). Um formato de antena bastante conveniente para radiotelescópios se dá no formato parabólico, pois a radiação se concentra em um único ponto, onde fica o alimentador. O campo de visão ou resolução do radiotelescópio é um fator fundamental a ser considerado no projeto, dependendo do tipo de observação que será realizada. A unidade

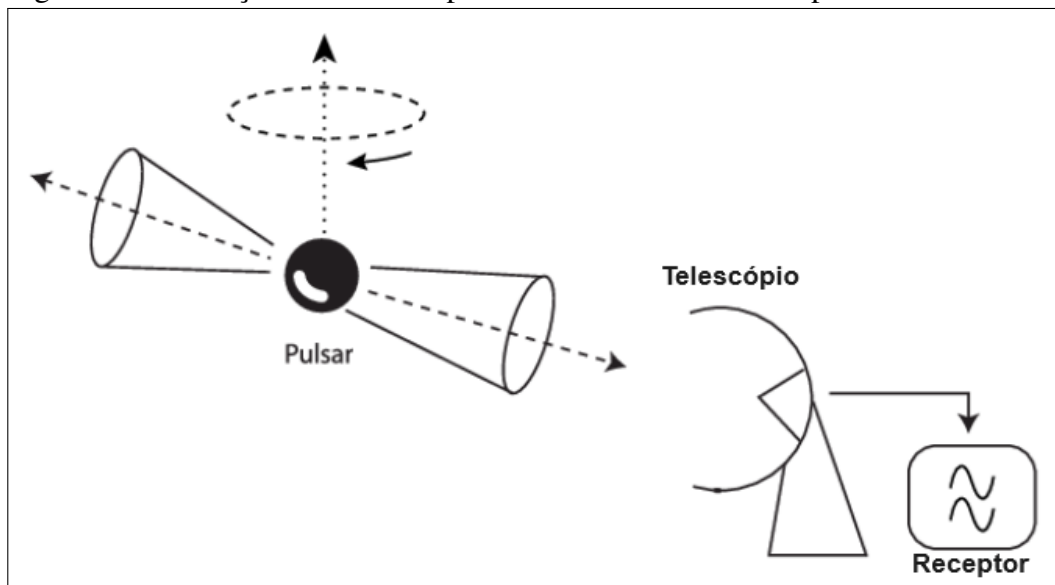
Figura 9 – Interpulso em PSR B1702-19 (1,4GHz)



Fonte: adaptado de (LYNE; GRAHAM-SMITH, 2012).

de densidade de fluxo espectral na radioastronomia é o Jansky (Jy). Ele é expresso em termos de potência recebida por unidade de área de coleta e largura de banda, $1\text{Jy} = 10^{-26}\text{Wm}^{-2}\text{Hz}^{-1}$ (LORIMER; KRAMER, 2004).

Figura 10 – Detecção de sinais de pulsares usando radiotelescópios



Fonte: adaptado de (LORIMER; KRAMER, 2004).

Considera-se a observação de uma fonte de rádio não polarizada com densidade de

fluxo 'S' utilizando um radiotelescópio de área efetiva $A_e = \eta A$, onde A é a área da antena e η representa a eficiência do telescópio. Cada modo de polarização contribui pela metade para o fluxo total, portanto a potência recebida da fonte por unidade de largura de banda e polarização é $P_{fonte} = (SA_e)/2$. Frequentemente é útil na radioastronomia utilizar o conceito de "temperatura de antena" (T_A). Para isto, considera-se substituir uma antena por um circuito contendo um elemento de resistência a uma temperatura T . Movimentos térmicos aleatórios de elétrons induzem neste circuito uma tensão variável com o tempo, que de acordo com o teorema de Nyquist produz uma potência por unidade de largura de banda dada por $P_{circuito} = k_B T$, onde k_B é a constante de Boltzmann. Desta forma, substituindo-se T por T_A relaciona-se a densidade de fluxo S com a temperatura da antena T_A através da eq.(3.1).

$$S = \frac{2k_B T_A}{A_e} = \frac{T_A}{G} \quad (3.1)$$

onde $G = A_e / (2K - B)$ é o ganho.

O ganho é determinado pela área efetiva da antena e mede a sensibilidade bruta desta. Desta forma sempre se pode pensar em uma fonte de fluxo S_{fonte} tendo uma temperatura de fonte equivalente $T_{fonte} = G(S_{fonte})$. Na prática, sistemas de observação reais têm muitas fontes de ruído, de modo que fontes fracas têm que lidar com uma "temperatura de sistema" T_{sis} de fundo dada pela eq. (3.2).

$$T_{sis} = T_{rec} + T_{spill} + T_{atm} + T_{ceu} \quad (3.2)$$

Na expressão (3.2), T_{rec} é o ruído de temperatura do receptor (tipicamente 20K para sistemas refrigerados), T_{spill} é o ruído "spillover", que é a contribuição do solo e está relacionado à elevação da antena, geralmente estando na ordem de 10K ou menos. T_{atm} se deve à emissão atmosférica (em geral, relevante apenas para frequências de observação acima de 5 GHz) e T_{ceu} se refere à radiação de fundo do céu. A fonte predominante deste último ruído é oriunda dos elétrons síncrotron radiantes no plano da Via Láctea. T_{ceu} é altamente dependente da posição celeste e frequência observacional. A 430MHz ele pode atingir 800K para observações direcionadas ao centro da galáxia (LORIMER; KRAMER, 2004). De acordo com Lyne e Graham-Smith (2012), um fator relevante para um planejamento de observações é o limite de sensibilidade. Um longo tempo de integração, em geral, garante uma alta sensibilidade, enquanto a menor periodicidade requer uma taxa de amostragem rápida. Estes dois fatores juntos são responsáveis

pelo número total de amostras em uma integração, que por sua vez é limitado pelas possibilidades de processamentos de dados. Em levantamentos amplos, para uma detecção significativa, a relação sinal-ruído (S/R) deve ser ajustada para um valor alto o suficiente para evitar muitas detecções falsas. Em um sistema com ganho de antena G , temperatura total de ruído T_{sis} , usando N_p canais de polarização ($N_p = 1$) ou ($N_p = 2$), a densidade mínima de fluxo S_{min} é dada pela eq. (3.3).

$$S_{min} = \frac{\alpha\beta}{(N_p\Delta\nu t_{int})^{1/2}} \left(\frac{W}{P-W} \right)^{1/2} \frac{T_{sis}}{G} \quad (3.3)$$

onde α é a relação sinal-ruído limiar, β é um fator de correção devido ao processo de digitalização e outras perdas no processamento do sinal (em geral, $\beta \gtrsim 1$). W é a largura do pulso efetiva e P é o período do pulso.

De acordo com Lyne e Graham-Smith (2012), a dificuldade inicial para reconhecimento e detecção dos sinais de rádio vindo dos pulsares era que os astrônomos não esperavam que qualquer corpo celeste pudesse emitir sinais com flutuações tão rápidas. Sinais de rádio em formatos de pulsos captados por radiotelescópios eram frequentemente confundidos com sinais advindos de dispositivos tecnológicos terrestres que poderiam emitir sinais periódicos, como máquinas elétricas, descargas de linhas de energia e ignição de automóveis. Outra interpretação era de que estes pulsos poderiam vir de rajadas elétricas atmosféricas. A maioria dos receptores de sinais de rádio foi projetada para ignorar sinais impulsivos, preservando somente sinais contínuos ao longo de um tempo razoável de integração da medição. Mesmo se um tempo de integração mais curto estivesse em uso, dados impulsivos que eventualmente pudessem aparecer nos gráficos dos instrumentos já seriam esperados, visto que poderiam ser interpretados como dispositivos simples tais como cercas elétricas em fazendas, como dito anteriormente. Contudo, as pesquisas que atuavam nesse tipo de detecção ainda não estavam trabalhando de forma sistematizada e portanto faltavam duas características importantes para que a real fonte destes pulsos fosse detectada: um tempo de resposta dos instrumentos suficientemente curto e uma rotina de observação repetitiva, que poderia mostrar que os sinais periódicos aparentemente oriundos de fontes terrestres, eram na verdade, provenientes de uma fonte celestial permanente. Esses foram ambos os recursos utilizados por Anthony Hewish no contexto em que o primeiro pulsar foi descoberto (LYNE; GRAHAM-SMITH, 2012).

O fenômeno de cintilação das estrelas visíveis, bastante comum e observado cotidianamente por pessoas de todo o mundo, se dá devido à refração caótica na atmosfera terrestre. Este

efeito é perceptível portanto na faixa de frequências visível. Existe também um fenômeno similar capaz de afetar as ondas de rádio. Esta refração aleatória, causando cintilação das ondas de rádio provenientes de fontes celestes, ocorre principalmente de três formas distintas: na ionosfera terrestre, no gás interplanetário ionizado no Sistema Solar e no gás interestelar ionizado da Via Láctea. Em todas as ocasiões, as ondas de rádio de uma fonte distante atravessam esses meios com flutuações do índice de refração suficientes para desviar os feixes de rádio de forma a interferir na observação, visto que se cruzam antes de chegarem aos instrumentos de medição. A teoria da cintilação interestelar é extremamente relevante para o estudo dos pulsares, devendo ser considerada no processo de observação. Coincidentemente, uma investigação da cintilação interplanetária levou, perifericamente, à descoberta dos pulsares (LYNE; GRAHAM-SMITH, 2012).

De acordo com Dawson (2022), para se perceber a cintilação é necessário que os telescópios estejam separados em escalas de milhares de quilômetros. Neste caso, pode haver variação na densidade de fluxo captada pelos radiotelescópios. Outro fenômeno que deve ser considerado na radioastronomia é a interferência de radiofrequência RFI. Este fenômeno é bastante problemático, pois como muitas vezes os sinais astronômicos são fracos em relação ao ruído, estes podem confundir o sistema de detecção e análise. Afim de evitar maiores interferências, algumas faixas de frequência são alocadas para a radioastronomia, tanto nacionalmente como internacionalmente. Mesmo que existam essas bandas protegidas, larguras de banda mais ampla muitas vezes são necessárias para observações mais sensíveis, como buscas por pulsares, por exemplo. Por esta razão os observatórios de radioastronomia são instalados em regiões remotas, com pouca atividade humana, porém, mesmo com estes cuidados, nenhum observatório pode evitar totalmente a RFI, principalmente as interferências provenientes de satélites artificiais em órbita. Outra maneira de se reduzir a influência desses sinais de interferência se dá através de filtros específicos de frequência de rádio nos amplificadores, calibrados de forma que não haja perda significativa da sensibilidade da observação (LYNE; GRAHAM-SMITH, 2012).

3.3 Utilização de Pulsares para Geração de Sinais Aleatórios

De acordo com Dawson (2022), pulsares podem ser excelentes fontes PVR (*publicly verifiable randomness*) físicas, visto que apresentam alguns comportamentos imprevisíveis. Algumas dessas características podem ser medidas a cada pulso, tais como o brilho e a forma do pulso, enquanto outras só podem ser medidas em um grande intervalo de tempo, como o período

de rotação (pulsares são conhecidos por serem relógios extremamente precisos). Estas condições são:

- a) **disponibilidade**: que garante que nenhuma das partes é capaz de bloquear o acesso à fonte aleatória pela outra parte;
- b) **imprevisibilidade**: nenhuma das partes é capaz de prever bits futuros;
- c) **inflexibilidade**: nenhuma das partes é capaz de influenciar na aleatoriedade de futuras sequências de dados;
- d) **verificabilidade pública**: quaisquer atores da comunicação podem verificar a exatidão dos bits gerados;
- e) **servidor não confiável**: não há necessidade de intermediação de ativação e gerenciamento de dados por parte de um servidor confiável.

Desta forma, verifica-se que a utilização de estrelas pulsares para geração de sequências aleatórias de bits satisfaz cinco condições imprescindíveis para um protocolo PVR . Quanto à **disponibilidade**, existem milhares de pulsares conhecidos e detectáveis de diferentes localidades do planeta Terra. Como o sinal destes é emitido em uma vasta faixa de frequências e não pode ser bloqueado diretamente na fonte, a sua disponibilidade é garantida de forma bastante satisfatória. Com relação à **imprevisibilidade**, testes formais de aleatoriedade podem assegurar que diversas propriedades dos pulsares podem ser utilizadas como fontes de sequências aleatórias. Por motivos óbvios, é impossível influenciar o comportamento futuro dos pulsares e é extremamente complicado para qualquer outra parte alterar a medição dos dados da terra, portanto verifica-se também a sua **inflexibilidade**. Por fim, qualquer parte do sistema de comunicação com um radiotelescópio e/ou outros instrumentos adequados podem verificar a exatidão dos dados gerados (**verificabilidade pública**) e a geração de dados aleatória não necessita de um intermediador confiável (**servidor não confiável**). Ainda neste contexto, é importante destacar que outros fenômenos físicos em geral, são opções promissoras para geração de números aleatórios. Alguns exemplos de fenômenos físicos que podem ser utilizados para esta finalidade são: difusão de partículas, turbulência atmosférica, caos na emissão de lasers, síntese de DNA, dentre outros (DAWSON, 2022). Embora tenha-se uma vasta gama de opções, a geração de sequências numéricas aleatórias baseadas em fenômenos físicos naturais locais não satisfazem todos os requisitos exigidos no protocolo PVR (DAWSON, 2022). Conforme descrito em Canetti (2007 apud (DAWSON, 2022)) outras fontes astronômicas poderiam ser utilizadas para gerar

aleatoriedade, tais como as manchas solares, dentre outras, porém a vantagem da utilização dos pulsares é que seu sinal está disponível durante o dia e à noite.

4 FUNÇÃO LAMBERT-TSALLIS (W_q)

A função W de Lambert é a solução da eq. 4.1. Ela é utilizada para resolver analiticamente diversos problemas em Física, Ciências da Computação e Matemática. (SILVA; RAMOS, 2019).

$$W(z) \cdot e^{W(z)} = z, \quad (4.1)$$

Tsallis , utilizando as q -operações, descritas nas eqs. 4.2, 4.3, 4.4, 4.5 e 4.6, introduziu a entropia descrita na eq. 4.7, generalizando assim a mecânica estatística de Boltzmann-Gibbs (STEINBERG; TSALLIS; UMAROV, 2008). Esta teoria é frequentemente chamada de **mecânica estatística não extensiva** e volta à sua forma padrão (mecânica estatística de Boltzmann-Gibbs) fazendo $\lim_{q \rightarrow 1} S_q$ na eq. 4.7.

$$a +_q b = a + b + (1 - q)ab, \quad (4.2)$$

$$a -_q b = \frac{(a - b)}{[1 + (1 - q)b]}, \quad (4.3)$$

$$a \times_q b = \max \left\{ \left[a^{(1-q)} + b^{(1-q)} - 1 \right]^{[1/(1-q)]}, 0 \right\} = \left[a^{(1-q)} - b^{(1-q)} - 1 \right]_+^{[1/(1-q)]}, \quad (4.4)$$

$$a /_q b = \left[a^{(1-q)} - b^{(1-q)} + 1 \right]_+^{[1/(1-q)]}, \quad (4.5)$$

$$e_q^z = \begin{cases} [1 + (1 - q)z]^{1/(1-q)}, & q \neq 1 \text{ \& } 1 + (1 - q)z \geq 0 \\ 0, & q \neq 1 \text{ \& } 1 + (1 - q)z < 0. \end{cases} \quad (4.6)$$

$$S_q = \frac{1 - \sum_i p_i^q}{q - 1}, \quad (4.7)$$

A função W_q de Lambert-Tsallis é uma generalização da função Lambert W e pode ser usada para resolver algumas equações não lineares nas quais variáveis dependentes e independentes são relacionadas por uma lei de potência. A definição da função Lambert-Tsallis W_q está descrita na eq. 4.8 e é semelhante à definição da função de Lambert (SILVA; RAMOS, 2019).

$$W_q(z) \cdot e_q^{W_q(z)} = z \quad (4.8)$$

contudo, como pode ser visto nas eqs. 4.6 e 4.8, ela usa a função q -exponencial generalizada (TSALLIS, 1988). Como $\lim_{q \rightarrow 1} e_q^x = e^x$ tem-se $\lim_{q \rightarrow 1} W_q(z) = W(z)$. Por exemplo, para $q = 2$ e $q = 3/2$ têm-se as seguintes fórmulas analíticas para $W_q(z)$ descritas em (4.9) e (4.10).

$$W_2(z) = \frac{z}{z+1}, \quad z > -1, \quad (4.9)$$

$$W_{3/2}^{\pm}(z) = \frac{2(z+1) \pm 2\sqrt{2z+1}}{z}, \quad z > -1/2. \quad (4.10)$$

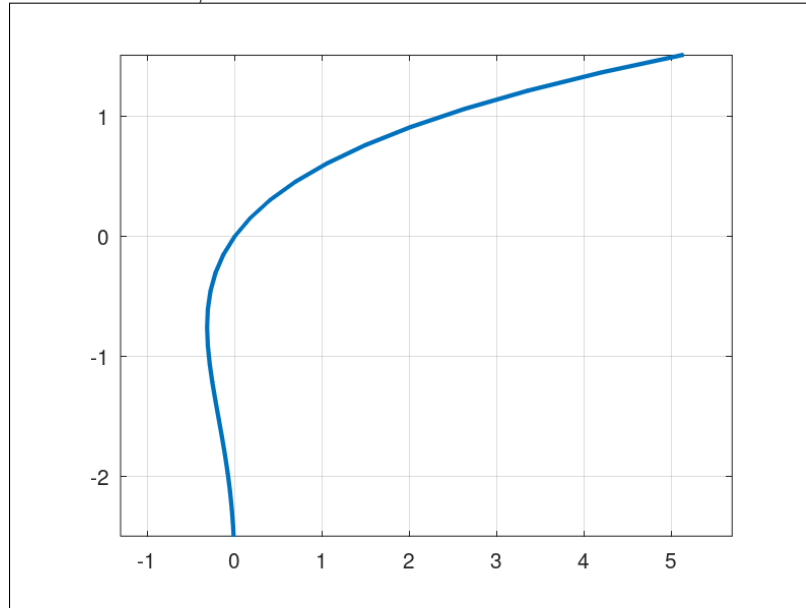
Como se pode notar na eq.4.10, em geral, W_q tem duas soluções reais (e muitas soluções complexas não descritas neste estudo) e elas se encontram no ponto de ramificação $\{z_b = \exp_q(1/(q-2))/(q-2), W_q(z_b) = 1/(q-2)\}$. Uma vez que só é possível encontrar uma expressão analítica para alguns poucos valores de q , a função Lambert-Tsallis $W_q(z)$ pode ser calculada através de procedimentos numéricos, como o método de Halley (SILVA; RAMOS, 2019). Neste caso, podem-se usar os seguintes mapas (4.11) e (4.12):

$$w_q(j+1) = w_q(j) - \frac{\left[w_q(j) e_q^{w_q(j)} - z \right]}{\left[e_q^{w_q(j)} + w_q(j) e_{2-\frac{1}{q}}^{q w_q(j)} \right] - \Lambda} \quad (4.11)$$

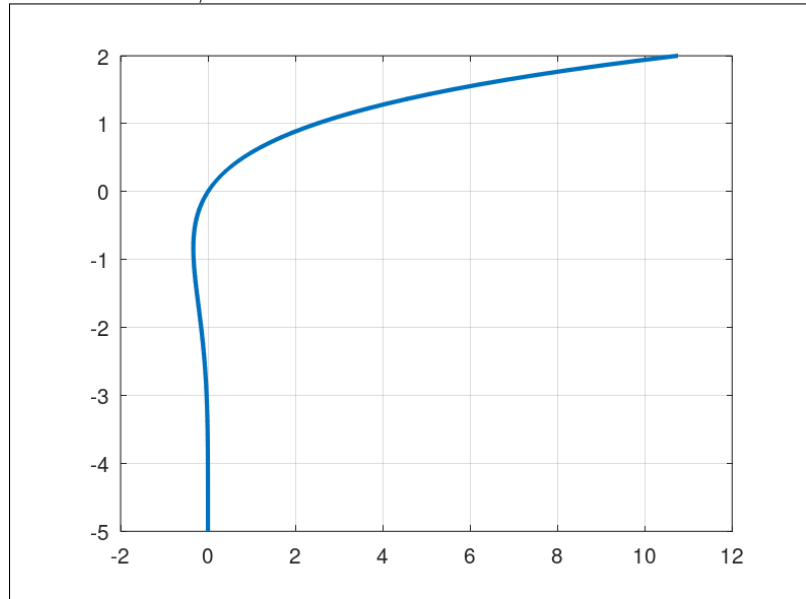
$$\Lambda = \frac{\left[w_q(j) e_q^{w_q(j)} - z \right] \left[2 e_{2-\frac{1}{q}}^{q w_q(j)} + \frac{w_q(j)}{q} e_{\left(\frac{3-2/q}{2-1/q}\right)}^{(2q-1)w_q(j)} \right]}{2 \left[e_q^{w_q(j)} + w_q(j) e_{2-\frac{1}{q}}^{q w_q(j)} \right]} \quad (4.12)$$

A convergência dos mapas (4.11) e (4.12) depende do valor inicial usado para $W_q(z)$. Por exemplo, nas Figuras 11 e 12 pode-se ver os gráficos de $W_{2/3}(z)$ versus z e $W_{4/5}(z)$ versus z .

Mais detalhes e aplicações da função W_q de Lambert-Tsallis podem ser encontrados em (ANDRADE; NOBREGA; RAMOS, 2021; RAMOS, 2022; GUEDES; NOBREGA; RAMOS, 2022).

Figura 11 – $W_{2/3}(z)$ versus z 

Fonte: o autor.

Figura 12 – $W_{4/5}(z)$ versus z 

Fonte: o autor.

4.1 Disentropia

A disentropia é um novo conceito que foi introduzido em Silva e Ramos (2019). Basicamente, a disentropia é o oposto da entropia: a disentropia é máxima para uma distribuição delta e mínima para uma distribuição uniforme, enquanto ocorre o oposto com a entropia. Enquanto a entropia generalizada é baseada na função $\log q$ de Tsallis (eq.4.13), a disentropia generalizada é baseada na função W_q de Lambert (eq.4.8). As disentropias discretas e contínuas são simplesmente dadas pelas eqs. 4.14 e 4.15 (SILVA; RAMOS, 2019).

$$l_{n_q}(z) = \begin{cases} \ln(z) & \text{se } z > 0 \text{ e } q = 1 \\ \frac{z^{(1-q)} - 1}{1-q} & \text{se } z > 0 \text{ e } q \neq 1 \\ \text{indefinido} & \text{se } z \leq 0 \end{cases} \quad (4.13)$$

$$D_q = \sum_i p_i^q W_q(p_i) \quad (4.14)$$

$$D_q = \int_{-\infty}^{\infty} p^q(x) W_q(p(x)) dx \quad (4.15)$$

onde (p_i) é uma distribuição de probabilidade discreta, e $(p(x))$ é uma distribuição contínua.

A princípio, pode-se imaginar que a utilização da entropia ou disentropia são apenas pontos de vistas diferentes para uma mesma situação, e a escolha para usar uma ou outra seja puramente arbitrária, porém neste caso, há diferenças na utilização de uma ou outra. Como $W_q(z)$ é real para valores negativos de z ($z \geq z_b$), a disentropia pode ser utilizada em situações nas quais a entropia não pode ser utilizada. Em Ramos (2021), a disentropia da função de autocorrelação é utilizada como parâmetro de medida de aleatoriedade. A disentropia da autocorrelação, portanto, pode ser utilizada para medir a aleatoriedade de sinais discretos s_t e sinais contínuos $s(t)$. Por exemplo, para $q = 2$, os valores são respectivamente:

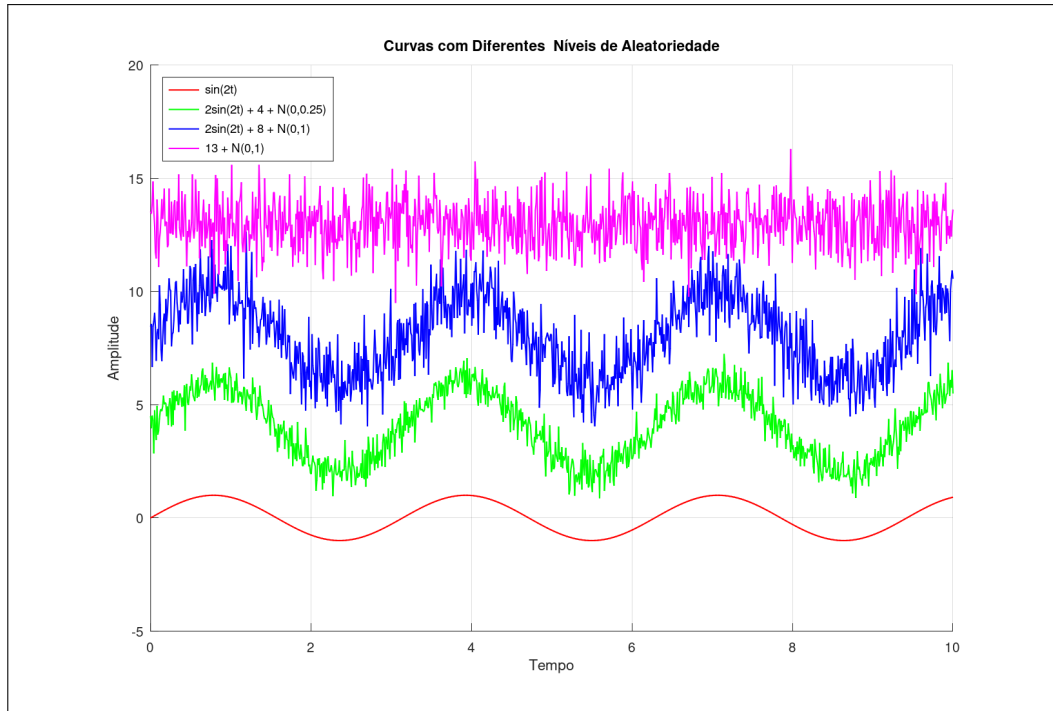
$$D_2 = \sum_{n=1}^N \frac{r_n^3}{r_n + 1} \quad (4.16)$$

$$D_2 = \int_{-\infty}^{\infty} \frac{R^3(\tau)}{R(\tau) + 1} d\tau, \quad (4.17)$$

onde r_n é o n -ésimo valor da função discreta de autocorrelação de s_t e $R(\tau)$ é a função de autocorrelação do sinal contínuo $s(t)$. Um sinal discreto, puramente aleatório, cuja função de autocorrelação é a função delta com magnitude igual a 1, tem $D_2 = 0,5$. Desta forma, quanto mais próxima de 0,5 for a disentropia da autocorrelação, maior é a quantidade de aleatoriedade. Diferente de outras metodologias para medição de aleatoriedade, que eventualmente podem aferir se uma sequência é ou não aleatória, a disentropia, neste caso, pode fornecer um gradiente de medida de aleatoriedade. Conforme verifica-se na Figura 13, têm-se quatro curvas: a primeira

é periódica, a segunda e terceira são compostas (periódica + aleatória) e a quarta é puramente aleatória. Estas curvas podem representar diferentes sinais com diferentes níveis de aleatoriedade conforme verifica-se na Tabela 3.

Figura 13 – Sinais com diferentes níveis de aleatoriedade



Fonte: adaptado de (ALMEIDA; RAMOS, 2022).

Tabela 3 – Disentropia de sinais periódicos e/ou aleatórios

Curva	S(t)	D ₂ (S(t))
1	2sin(t)	427,5291
2	2sin(t) + 4 + N (0,0,25)	174,3615
3	2sin(t) + 8 + N (0,1)	30,2728
4	13 + N (0,1)	0,4917

Fonte: adaptado de (ALMEIDA; RAMOS, 2022).

A disentropia também pode ser utilizada para medir a distância entre distribuições de probabilidade. Neste caso, deve ser utilizada a disentropia relativa (RAMOS, 2019; SILVA; RAMOS, 2020) cujas versões discretas e contínuas são dadas por:

$$D_q = \langle p(x) \| q(x) \rangle = \sum_i p_i^q |W_q(p_i) - W_q(q_i)| \quad (4.18)$$

$$D_q = \langle p(x) \| q(x) \rangle = \int_x p^q(x) |W_q(p(x)) - W_q(q(x))| dx. \quad (4.19)$$

onde, nas eqs. 4.18 e 4.19, $p(x)$ and $q(x)$ são distribuições de probabilidade.

5 SIMULAÇÃO NUMÉRICA DE UMA DISTRIBUIÇÃO DE CHAVES USANDO UM PULSAR

5.1 Parâmetros da Simulação

Como explicado no Capítulo 2, um pulsar é um estrela de nêutrons em rotação, oriunda geralmente de uma explosão de supernova que emite uma intensa radiação eletromagnética perpendicularmente aos seus polos magnéticos. A captação desta radiação se dá no momento em que estes polos estão apontados para a Terra. A frequência de emissão destes pulsos é dependente do período de rotação de cada pulsar, que pode variar de segundos a milissegundos. Conforme dito anteriormente nos Capítulos 2 e 3, a natureza aleatória destes pulsos pode ser utilizada para geração de sequências de bits aleatórios, que por sua vez podem ser utilizadas para geração de chaves para vários esquemas criptográficos, como uma cifra de Vernam, por exemplo. De acordo com Mickaliger *et al.* (2018), a maioria dos pulsares emite sinais de rádio, cuja densidade de fluxo segue uma distribuição log-normal. A função densidade de probabilidade (PDF) deste fluxo é descrita pela eq. 5.1:

$$PDF_{ln}(E) = \frac{C}{E\sigma\sqrt{2\pi}} e^{-\frac{[\ln(E) - \mu]^2}{2\sigma^2}} \quad (5.1)$$

onde C é uma constante de normalização. Os parâmetros $\mu = 0,1648$ e $\sigma = 0,5733$ da PDF utilizados são característicos do pulsar (PSR J0437-4715) (ALMEIDA; RAMOS, 2022). Para se estabelecer uma boa simulação, considera-se que em geral, o sinal medido pelos dois radiotelescópios das duas partes é uma composição do sinal do próprio pulsar considerado, do ruído gaussiano intrínseco e exclusivo de cada telescópio, e outros sinais vindos de galáxias, nuvens moleculares, radiação cósmica de fundo, dentre outras. Neste trabalho consideraram-se apenas o sinal dos pulsares e o ruído normal dos radiotelescópios, visto que estes correspondem à maior parcela dos sinais mencionados. Há de se considerar também que embora o ruído gaussiano intrínseco dos instrumentos de medição não possa ser filtrado, outros ruídos mencionados podem ser minimizados e/ou eliminados através de diversas técnicas. Considerando a composição mencionada, descreve-se nas eqs. 5.2 e 5.3, os sinais completos medidos por Alice (y_n^A) e Bob (y_n^B).

$$y_n^A = \xi_n + \varepsilon_n^A \quad (5.2)$$

$$y_n^B = \xi_n + \varepsilon_n^B. \quad (5.3)$$

Nas eqs. (5.2) e (5.3), ξ_n é a n -ésima amostra da densidade de fluxo que segue a PDF descrita em (5.1). Estes termos obviamente são iguais para Alice e Bob pois se tratam do sinal eletromagnético advindo da estrela pulsar. Os termos ε_n^A e ε_n^B são as n -ésimas amostras dos ruídos gaussianos $\mathcal{N}(0, \sigma^2)$ inseridos por cada radiotelescópio de Alice e Bob, sendo portanto, diferentes. Como ε_n^A and ε_n^B são ruídos independentes, Alice e Bob, eventualmente irão finalizar a extração de bits com chaves diferentes. De acordo com Dawson (2022), o método de extração de bits com a maior taxa de transmissão de bits confidenciais se daria estabelecendo-se limiares e simplesmente fazendo-se a comparação dos sinais capturados $y_n^{A(B)}$ com a mediana $m_{A(B)}$ de $y^{A(B)}$: neste caso, a chave receberia um bit '1' quando o sinal ultrapassar a mediana (limiar) $y^{A(B)} \geq m_{A(B)}$ e receberia o valor '0' quando ocorresse o contrário. Neste trabalho, considerou-se um cenário em que o ruído corresponde a cerca de 25% do sinal útil do pulsar, portanto, a taxa de erro é dependente da variância do ruído gaussiano. Neste caso, por exemplo, para $\sigma \sim 0,25$ tem-se uma taxa de erro de bits (BER) $\sim 15\%$. Conforme descrito em Gisin *et al.* (2002), esta taxa é maior que o limite de 11%, definido pela expressão (5.4), desta forma, impedindo o estabelecimento de uma chave comum entre Alice e Bob.

$$BER \log_2(BER) + (1 - BER) \log_2(1 - BER) \leq \frac{1}{2} \quad (5.4)$$

onde BER é a taxa de erro ($BER \leq 11\%$).

5.2 Aplicação do Algoritmo para Diminuição da Taxa de Erro

A fim de se estabelecer uma chave válida, e portanto, diminuir a taxa de erro de bits, propõe-se o seguinte algoritmo que deve ser executado por Alice e Bob de forma independente:

Input (y) (o vetor com os dados medidos)

I – Define-se uma distribuição de referência log-normal:

$$PDF_{ref}(y) = \frac{C_{ref}}{y\sigma_{ref}\sqrt{2\pi}} e^{-\frac{[\ln(y) - \mu_{ref}]^2}{2\sigma_{ref}^2}} \quad (5.5)$$

Onde μ_{ref} = média amostral de y e σ_{ref} = variância amostral de y $1/2$.

Define-se m = mediana(y).

II - **for** $k = 1:200$,

II.1 - Usa-se o histograma de y para estimar a distribuição de y : $PDF_{est}(y)$

$$[PDF_{est}(y_1)] = \text{hist}(y, 100)$$

II.2 – Calcula-se:

$$\Delta = D_2(PDF_{est}(y_1) | PDF_{ref}(y_1, \mu_{ref}, \sigma_{ref})) - D_2(PDF_{ref}(y_1, \mu_{ref}, \sigma_{ref})) :$$

$$\Delta = \sum_n \frac{[PDF_{ref}(y_1(n), \mu_{ref}, \sigma_{ref})]^2 PDF_{est}(y_1(n))}{1 + PDF_{est}y_1(n)} \quad (5.6)$$

II.3 - Atualiza-se o valor de y de acordo com a eq. 5.7:

$$y_n = y_n + \alpha \Delta y_{n-1} \quad (5.7)$$

Endfor

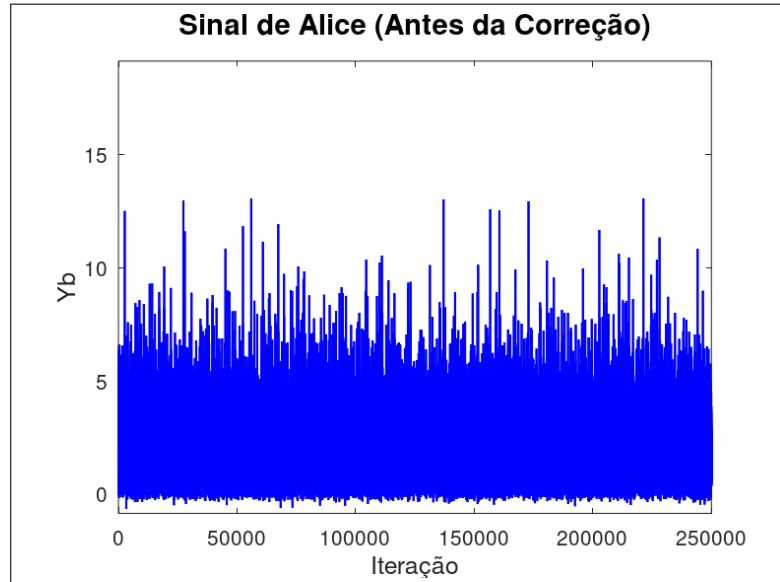
Na simulação foram utilizados $\alpha = 10$ e $k = 200$. Estes valores foram definidos empiricamente de forma a otimizar o algoritmo, visto que ganhos progressivos na diminuição da taxa de erro ao utilizar-se um coeficiente de correção α diferente ou mesmo aumentar-se o número de laços ($k > 200$) resultava em um aumento de tempo computacional. Os dados iniciais de Alice e Bob são obtidos através da eq. 5.8:

$$y_n^{A(B)} = \xi_n + 0,25 \mathcal{N}^{A(B)}(0, 1), \quad (5.8)$$

onde, de acordo com Almeida e Ramos (2022), ξ_n é estabelecido aleatoriamente de acordo com uma PDF log-normal com os parâmetros já mencionados $\mu = 0,1648$, $\sigma = 0,5733$ e $\mathcal{N}^{A(B)}(0, 1)$

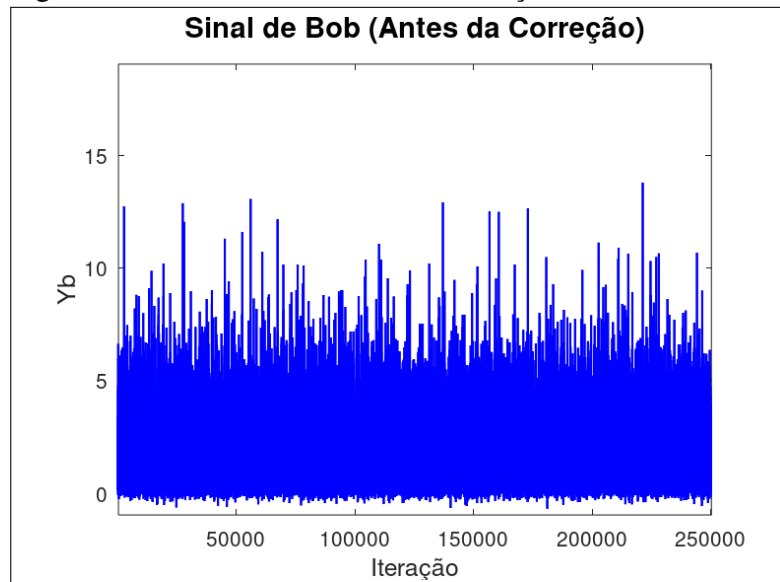
é uma distribuição normal padrão de parâmetros $\mu = 0$ e $\sigma = 1$. Dois vetores (Figuras 14 e 15) com 250000 elementos cada são produzidos de acordo com a eq. (5.8), constituindo portanto o tamanho inicial da chave criptográfica.

Figura 14 – Sinal de Alice antes da correção



Fonte: o autor.

Figura 15 – Sinal de Bob antes da correção

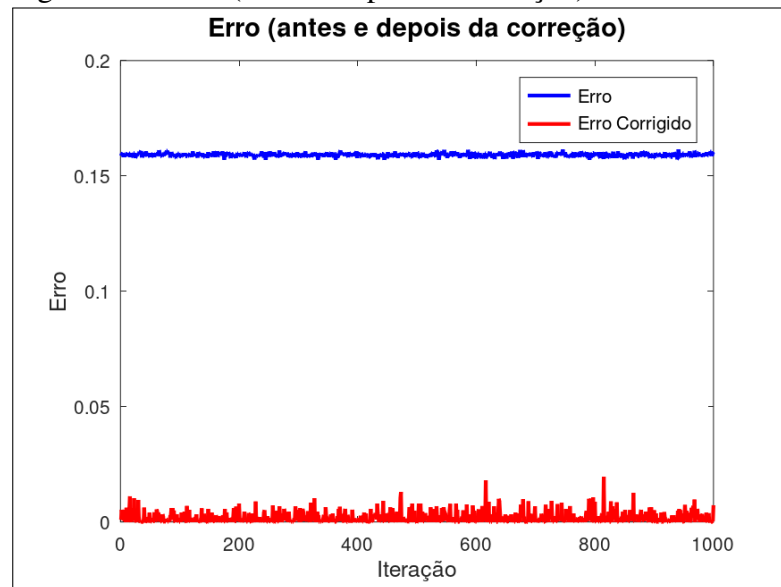


Fonte: o autor.

Conforme dito anteriormente, a extração de bits foi estabelecida como: bit '1' se $y_n \geq m$ e bit '0' se $y_n < m$. O resultado das simulações pode ser visto nas Figuras 16, 17, 18, 19, 20, 21, 22, 23 e 24. Na Figura 16 pode-se ver o BER antes (curva superior) e depois da correção (curva abaixo) aplicada pelo algoritmo após mil simulações. Pode-se ver claramente na Figura

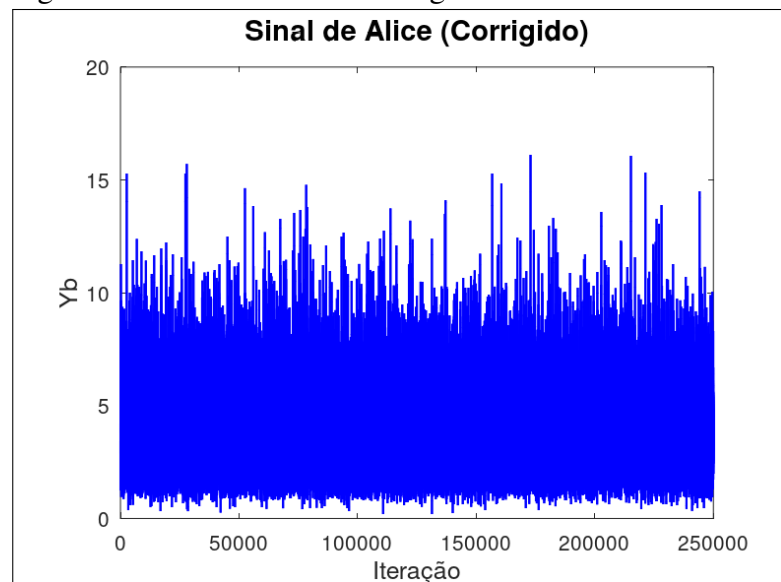
16 que a correção executada pelo algoritmo proposto diminuiu a taxa de erro de bits em torno de dezenas de vezes. No pior resultado das simulações a diminuição do erro ainda foi cerca de 8 vezes (Figura 16). Nas Figuras 17 e 18 podemos observar claramente a semelhança do padrão das chaves de Alice e Bob após a correção.

Figura 16 – Erro (antes e depois da correção)



Fonte: o autor.

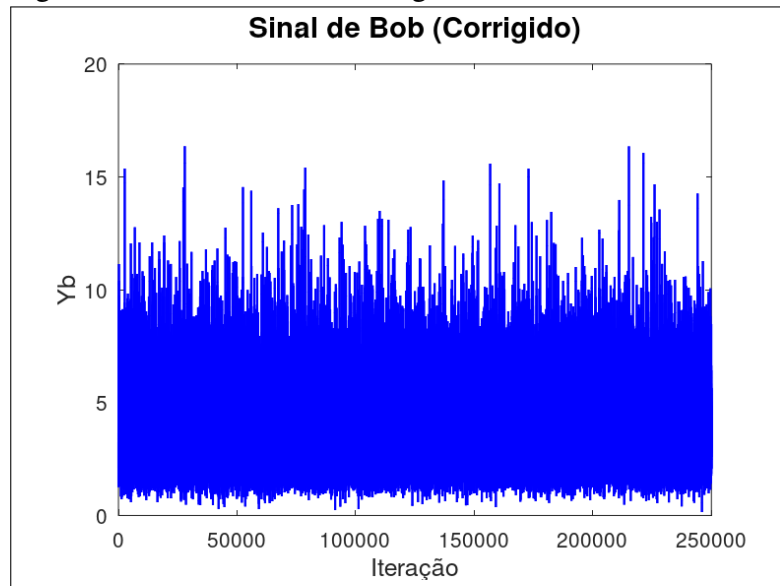
Figura 17 – Chave de Alice corrigida



Fonte: o autor.

Como mencionado anteriormente, um requisito bastante relevante para a validação das chaves criptográficas geradas é que estas mantenham a sua aleatoriedade. Neste sentido, as Figuras 19, 20, 21 e 22, mostram que a aleatoriedade das chaves não é afetada pela correção. Nas Figuras

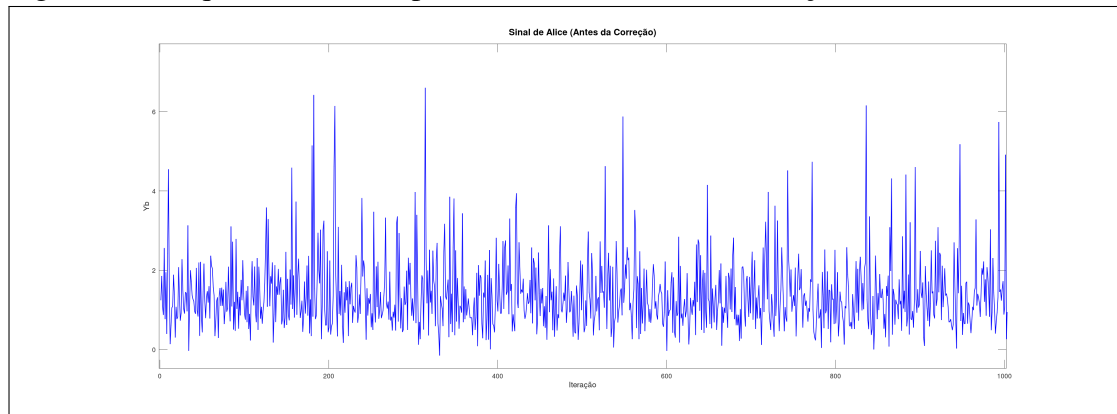
Figura 18 – Chave de Bob corrigida



Fonte: o autor.

19 e 20 podemos observar 1000 pontos do vetor y representando, para uma mesma simulação, as chaves de Alice antes e depois da correção, respectivamente. O mesmo aspecto pode ser observado nas chaves geradas por Bob.

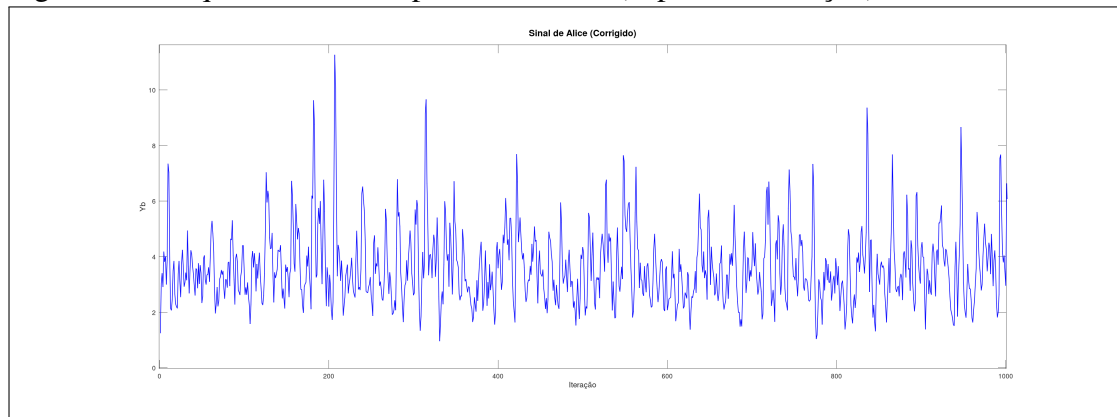
Figura 19 – Sequência de 1000 pulsos de Alice (antes da correção)



Fonte: o autor.

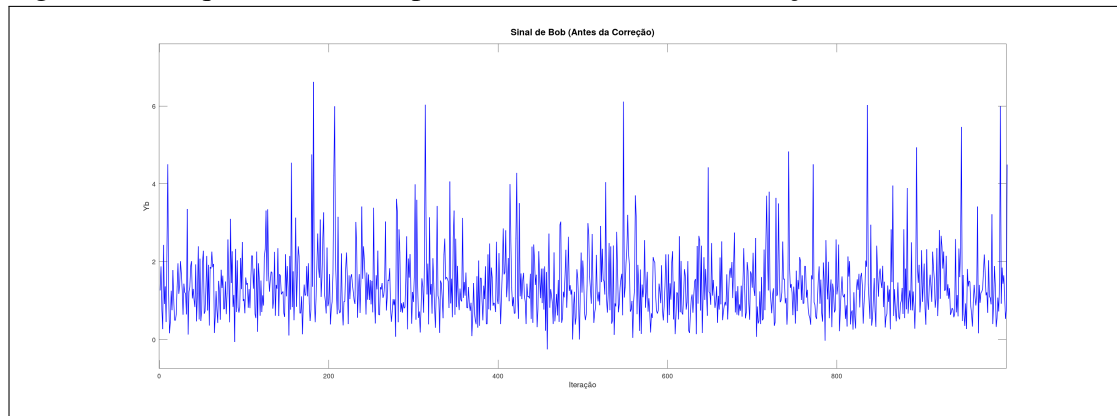
As Figuras 23 e 24 mostram os histogramas da aleatoriedade das chaves de Alice e Bob, representando a disentropia da autocorrelação calculada pelo algoritmo usando a eq. (4.16). Os histogramas também foram obtidos após a aplicação do algoritmo em 1000 simulações. Os valores da disentropia D_2 próximos de 0,5 nas distribuições de frequências mostradas nas Figuras 23 e 24 demonstram que as chaves permanecem com um alto índice de aleatoriedade. Após a execução do algoritmo (Apêndice A) mil vezes, em uma das simulações se pôde perceber que a taxa de erro média diminuiu aproximadamente 90 vezes, conforme mostra a Tabela 4. Os principais resultados da execução do algoritmo são a drástica diminuição da taxa de erro

Figura 20 – Sequência de 1000 pulsos de Alice (depois da correção)



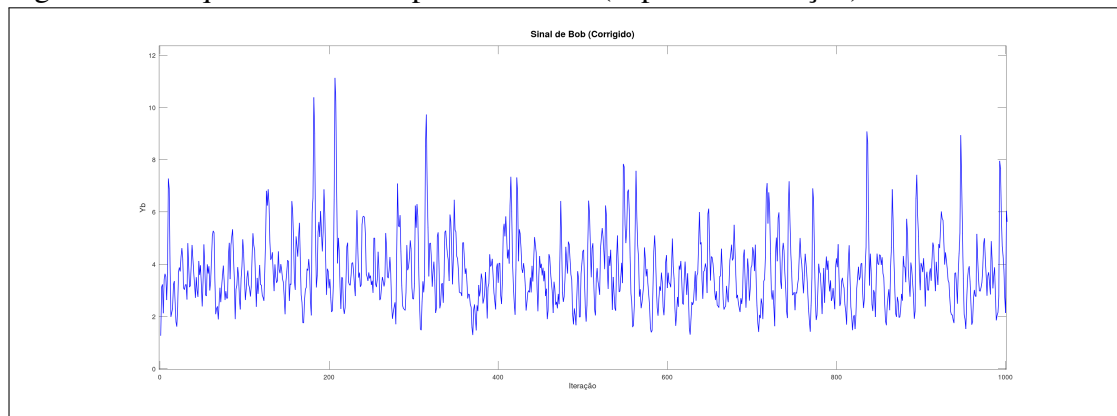
Fonte: o autor.

Figura 21 – Sequência de 1000 pulsos de Bob (antes da correção)



Fonte: o autor.

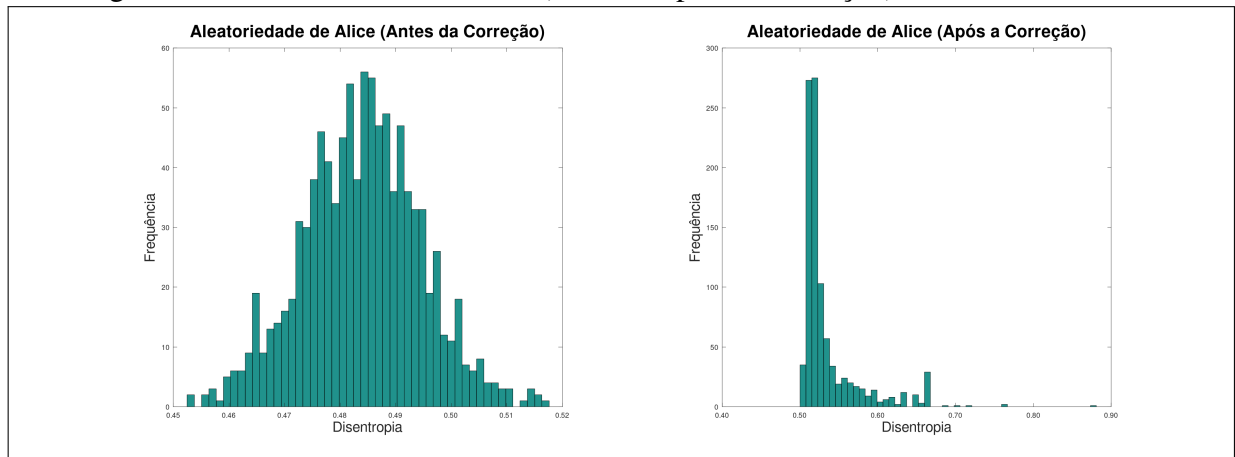
Figura 22 – Sequência de 1000 pulsos de Bob (depois da correção)



Fonte: o autor.

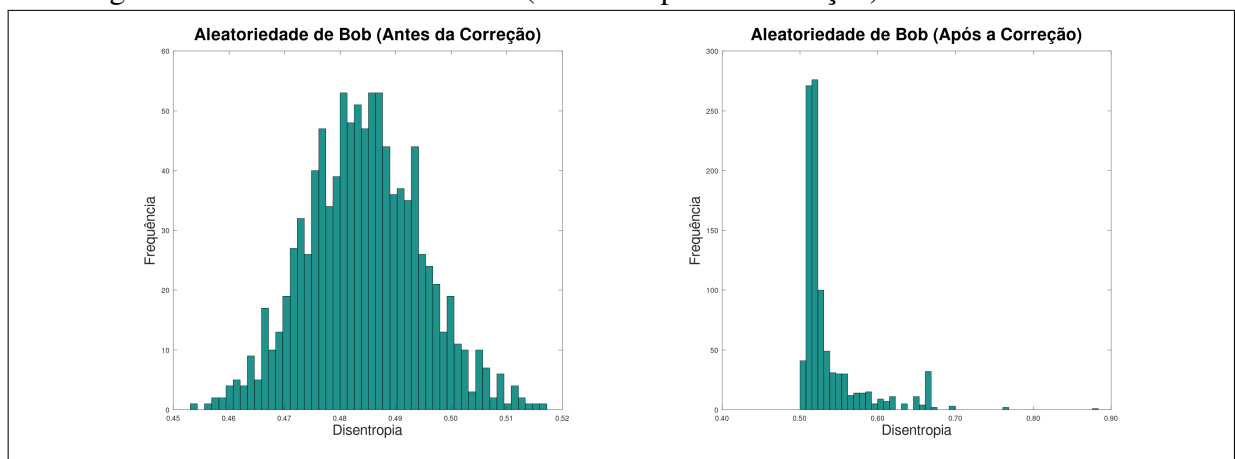
de bits entre Alice e Bob, bem como a verificação da manutenção da aleatoriedade da chave gerada. Esta última verificação é importante, pois a correção dos bits poderia eventualmente causar uma perda de aleatoriedade. Nas tabelas 5, 6 e 7 tem-se um exemplo dos dois primeiros e dois últimos resultados de uma execução do algoritmo:

Figura 23 – Aleatoriedade de Alice (antes e depois da correção)



Fonte: o autor.

Figura 24 – Aleatoriedade de Bob (antes e depois da correção)



Fonte: o autor.

Tabela 4 – BER média (antes e depois da correção)

ct	Média do erro antes da correção	Média do erro após a correção
1 a 1000	0,159123	0,001781

Fonte: o autor.

Tabela 5 – BER (antes e depois da correção)

ct	Erro antes da correção	Erro após a correção
1	0,15982	0,000108
2	0,1585	0,000084
...	...	...
999	0,15962	0,002292
1000	0,15894	0,000064

Fonte: o autor.

Tabela 6 – Aleatoriedade de Alice (antes e depois da correção)

ct	Aleatoriedade antes da correção	Aleatoriedade após a correção
1	0,50001	0,58718
2	0,49998	0,56928
...	...	...
999	0,49998	0,52087
1000	0,49997	0,58176

Fonte: o autor.

Tabela 7 – Aleatoriedade de Bob (antes e depois da correção)

ct	Aleatoriedade antes da correção	Aleatoriedade após a correção
1	0,49998	0,56436
2	0,49998	0,6071
...	...	...
999	0,5	0,51364
1000	0,49998	0,61902

Fonte: o autor.

6 CONCLUSÃO E PERSPECTIVAS FUTURAS

6.1 Conclusão

O algoritmo proposto para diminuição da taxa de erro dos bits de uma chave criptográfica usando pulsares diminuiu a taxa de erro (inicialmente de 15%) em média em 90 vezes, permitindo uma troca de chaves válida. Este algoritmo se baseou no princípio de que a disentropia evidenciada no texto é uma ferramenta eficaz de verificação da distância entre duas distribuições de probabilidades. Utilizando a disentropia da autocorrelação, verificou-se também a manutenção da aleatoriedade das chaves geradas, através do cálculo do valor da disentropia da autocorrelação da chave corrigida, que permaneceu próxima ao valor de "0,5" após as correções.

6.2 Perspectivas Futuras

Sugere-se para trabalhos futuros: I) a implementação deste algoritmo em diferentes fontes de dados aleatórios no universo: outros pulsares, manchas solares e radiação cósmica de fundo. II) Utilizar a disentropia da autocorrelação para comparar a aleatoriedade entre diferentes fenômenos cósmicos.

REFERÊNCIAS

- ALMEIDA, F. J. L.; RAMOS, R. V. Disentropy in Astronomy. **SSRN**, 2022. ISSN 0035-8711.
- ANDRADE, J. S. de; NOBREGA, K. Z.; RAMOS, R. V. Analytical solution of the current-voltage characteristics of circuits with power-law dependence of the current on the applied voltage using the Lambert-Tsallis W_q function. **IEEE Trans. on Circ. and Syst. II: Express Briefs**, IEEE, 2021.
- CHEN, J.-P.; ZHANG, C.; LIU, Y.; JIANG, C.; ZHANG, W.-J.; HAN, Z.-Y.; MA, S.-Z.; HU, X.-L.; LI, Y.-H.; LIU, H.; ZHOU, F.; JIANG, H.-F.; CHEN, T.-Y.; LI, H.; YOU, L.-X.; WANG, Z.; WANG, X.-B.; ZHANG, Q.; PAN, J.-W. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. **Nature Photonics**, v. 15, p. 570–575, 2021.
- COSTA, C. **Introdução à Criptografia. v1**. Rio de Janeiro-RJ: UFF / CEP – EB, 2010. v. 1. 100 p. ISBN 85-7648-303-3.
- DAWSON, J. R. Physical publicly verifiable randomness from pulsars. **Astronomy and Computing**, v. 38, p. 100549/1–10, 2022.
- FISCELLA, V. S.; PALACIO, S. del; COMBI, C. O. L. L.; COMBI, J. A.; GANCIO, G.; GARCÍA, F.; GUTIÉRREZ, E.; HAUSCARRIAGA, F.; KORNECKI, P.; ARMENGOL, F. G. L.; MANCUSO, G. C.; MÜLLER, A. L.; BUNZEL, A. S. Psrj0437-4715:theargentineinstituteofradioastronomy2019–2020observational campaign. **The Astrophysical Journal**, v. 908, n. 2, Fevereiro 2021.
- FRÖHLICH, B.; DYNES, J. F.; LUCAMARINI, M.; SHARPE, A. W.; TAM, S. W.-B.; YUAN, Z.; SHIELDS, A. J. Quantum secured gigabit optical access networks. **Scientific Reports**, v. 5, p. 18121/1–7, 2015.
- GISIN, N.; RIBORDY, G.; TITTEL, W.; ZBINDEN, H. Quantum cryptography. **Reviews of Modern Physics**, UNiversity of geneva, Geneva, v. 74, Março 2002.
- GUEDES, V. F.; NOBREGA, K. Z.; RAMOS, R. V. Analytical solution of the space charge limited current using the Lambert–Tsallis W_q Function. **IEEE Transactions on Electron Devices**, IEEE, 2022.
- LO, H.-K.; CURTY, M.; TAMAKI, K. Secure quantum key distribution. **Nature Photonics**, Cornell University Library, arXiv.org, Ithaca, v. 18, p. 595–604, 2014. ISSN 2331-8422.
- LORIMER, D. R.; KRAMER, M. **Handbook of Pulsar Astronomy**. Cambridge: Cambridge University Press, 2004. 312 p. (Cambridge Observing Handbooks for Research Astronomers, 4). ISBN 0521828236.
- LYNE, A.; GRAHAM-SMITH, F. **Pulsar Astronomy**. 4. ed. Cambridge: Cambridge University Press, 2012. 374 p. (Cambridge Astrophysics, 48). ISBN 978-1-107-01014-7.
- MICKALIGER, M. B.; MCEWEN, A. E.; MCLAUGHLIN, M. A.; LORIMER, D. R. A study of single pulses in the Parkes Multibeam Pulsar Survey. **Monthly Notices of the Royal Astronomical Society**, v. 479, n. 4, p. 5413–5422, 07 2018. ISSN 0035-8711.
- RAMOS, R. V. Disentropy of the Wigner function. **Journal of the Optical Society of America B**, v. 36, p. 2244–2249, 2019.

RAMOS, R. V. Estimation of the randomness of continuous and discrete signals using the disentropy of the autocorrelation. **SN Compt. Sci.** **2**, n. 254, 2021.

RAMOS, R. V. Analytical solutions of cubic and quintic polynomials in micro and nanoelectronics using the Lambert-Tsallis W_q function. **J. Comput. Electron.**, 2022.

SCARANI, V.; BECHMANN-PASQUINUCCI, H.; CERF, N. J.; DUŠEK, M.; LÜTKENHAUS, N.; PEEV, M. The security of practical quantum key distribution. **Rev. Mod. Phys.** **81**, p. 1301–1350, 2009.

SILVA, G. B. da; RAMOS, R. The Lambert-Tsallis W_q function. **Physica A**, v. 525, p. 164–170, 2019.

SILVA, J. L. E. da; RAMOS, R. V. Calculation of the disentropy of the Wigner function using the Lambert–Tsallis W_q function with non-integer q values. **Journal of the Optical Society of America B**, v. 37, n. 7, p. 2035–2040, 2020.

SOUSA, A. N. L. **Criptografia de Chave Pública, Criptografia RSA**. Dissertação (Mestrado), Rio Claro, 2013.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6. ed. São Paulo: Pearson, 2014. 560 p. ISBN 978-8543005898.

STEINBERG, S.; TSALLIS, C.; UMAROV, S. On a q -central limit theorem consistent with nonextensive statistical mechanics. **Milan Journal of Mathematics**, Birkhäuser Verlag Basel/Switzerland, 2008.

TSALLIS, C. Possible generalization of Boltzmann-Gibbs statistics. **Journal of Statistical Physics**, v. 52, p. 479–487, 1988.

ZOCHIO, M. F. **Introdução à Criptografia**. 1. ed. São Paulo: NOVATEC, 2016. 208 p. ISBN 978-85-7522-515-8.

APÊNDICE A – CÓDIGO DO ALGORITMO DE DIMINUIÇÃO DE TAXA DE ERRO (COMENTADO)

```

clear all

home

pkg load signal
pkg load statistics

%Parâmetros da função lognormal do pulsar
em=0.1648;s=0.5733;

%Define o tamanho da matriz utilizada.
tam=500;

% Inicializa vetores para armazenar os valores de erro e erro corrigido.

% Inicialize vetor para armazenar o erro.
Erro = zeros(1, 1000);

% Inicialize vetor para armazenar o erro corrigido.
Errop = zeros(1, 1000);

%Laço para alimentação dos vetores.
for ct=1:1000

%em=mu(média), s = sigma(desvio padrão), tam = tamanho do vetor(500 X 500).
aux=lognrnd(em,s,tam);

%y1= Distribuição lognormal do sinal da estrela.Tamanho do vetor (1 X 250000).
y1=reshape(aux,1,[]);
aux=normrnd(0,1,tam);

%y2= Distribuição lognormal do sinal de Alice (Gaussiano). Tamanho do vetor
(1 X 250000).
y2=reshape(aux,1,[]);
aux=normrnd(0,1,tam);

%y3= Distribuição lognormal do sinal de Bob (Gaussiano). Tamanho do vetor
(1 X 250000).
y3=reshape(aux,1,[]);

%Y1 Sinal completo gerador da chave de Alice.

```

```

Y1=y1+0.25*y2;
%Y2 Sinal completo gerador da chave de Bob.
Y2=y1+0.25*y3;
%YAb Backup do Sinal de Alice(Usado somente para plotar o sinal antes da correção).
YAb=y1+0.25*y2;
%YBb Backup do Sinal de Bob(Usado somente para plotar o sinal antes da correção).
YBb=y1+0.25*y3;
%Medianas dos sinais de Alice e Bob.
m1=median(Y1);m2=median(Y2);
%Cria dois vetores linhas nulos D1 e D2. Tamanho do vetor (1 X 250000).
D1=zeros(1,tam^2); D2=zeros(1,tam^2);
%Retorna um vetor de índices binários relativo aos sinais Y1 e Y2 cujos elementos
%valem 1 quando os respectivos valores de Y1 e Y2 ultrapassarem as medianas(
limiares m1 and m2).
D1(find(Y1>m1))=1;D2(find(Y2>m2))=1;
%Checa a diferença entre D1 e D2 antes da correção(em%)
Erro(ct)=length(find(xor(D1,D2)==1))/(tam^2);
% S1, S2 (Desvio padrão de Y1 e Y2)Em1, Em2 (Média de Y1 e Y2)
Em1=mean(Y1);S1=sqrt(var(Y1));Em2=mean(Y2);S2=sqrt(var(Y2));

%Laço de diminuição do erro

% 200 é um valor arbitrário para correção, definido empiricamente
for n=1:200,

%Alice

%Calcula o histograma do vetor Y1 com 100 bins. y1 contém as frequências de
cada bin e x1 contém os valores dos bins.
[y1 x1] = hist(Y1,100);
%Normaliza o vetor y1 para que a soma das frequências seja igual a 1;Calcula
os valores absolutos dos elementos em x1.
y1=y1/sum(y1);x1=abs(x1);

```

```

%Calcula a(PDF) da distribuição lognormal com média Em1 e desvio padrão S1.
Yref1=exp(-((log(x1)-Em1).^2)/(2*S1*S1))./(x1*S1*sqrt(2*pi));
%Normalização do vetor Yref1.
Yref1=Yref1/sum(Yref1);
%Calcula o valor de correção delta para Alice.
D21=sum(((Yref1.^2).*y1)./(1+y1));
% Yn Alice (corrigido);Atualiza o vetor Y1 com base no valor de correção D21.
Y1(2:tam*tam)=Y1(2:tam*tam)+10*D21*Y1(1:tam*tam-1);

%Bob

%Calcula o histograma do vetor Y2 com 100 bins. y2 contém as frequências de
cada bin e x2 contém os valores dos bins.
[y2 x2] = hist(Y2,100);x2=abs(x2);
%Normaliza o vetor y2 para que a soma das frequências seja igual a 1;Calcula
os valores absolutos dos elementos em x2.
y2=y2/sum(y2);
%Calcula a(PDF) da distribuição lognormal com média Em2 e desvio padrão S2.
Yref2=exp(-((log(x2)-Em2).^2)/(2*S1*S2))./(x2*S2*sqrt(2*pi));
%Normalização do vetor Yref2.
Yref2=Yref2/sum(Yref2);
%Calcula o valor de correção delta para Bob.
D22=sum(((Yref2.^2).*y2)./(1+y2));
% Yn Bob (corrigido);Atualiza o vetor Y2 com base no valor de correção D22.
Y2(2:tam*tam)=Y2(2:tam*tam)+10*D22*Y2(1:tam*tam-1);
end

%Resultados

% Calcula a mediana dos sinais após a correção
m1p=median(Y1);m2p=median(Y2);
%Cria dois vetores linhas nulos D1p e D2p. Tamanho do vetor (1 X 250000).
D1p=zeros(1,tam^2);D2p=zeros(1,tam^2);

```

```

%Retorna um vetor de índices binários relativo aos sinais Y1 e Y2 (corrigidos)cujos
elementos valem 1 quando os respectivos valores de Y1 e Y2 ultrapassarem as
medianas( limiares m1p and m2p).
D1p(find(Y1>m1))=1;D2p(find(Y2>m2))=1;
%Checa a diferença de bits entre D1 e D2 depois da correção (em%)
Errop(ct)=length(find(xor(D1p,D2p)==1))/(tam^2);
ct
%Erro (antes e depois da correção)
[Erro(ct) Errop(ct)];
disp(['Erro antes da correção: ' num2str(Erro(ct))]);
disp(['Erro depois da correção: ' num2str(Errop (ct))]);
Rand1(ct)=RandomnessImage(D1p,0);
Rand2(ct)=RandomnessImage(D2p,0);
% Aleatoriedade de Alice e Bob depois da correção
[Rand1(ct) Rand2(ct)];
disp(['Aleatoriedade de Alice depois da correção: ' num2str(Rand1(ct))]);
disp(['Aleatoriedade de Bob depois da correção: ' num2str(Rand2(ct))]);
Rand3(ct)=RandomnessImage(D1,0);
Rand4(ct)=RandomnessImage(D2,0);
% Aleatoriedade de Alice e Bob antes da correção
[Rand3(ct) Rand4(ct)];
disp(['Aleatoriedade de Alice antes da correção: ' num2str(Rand3(ct))]);
disp(['Aleatoriedade de Bob antes da correção: ' num2str(Rand4(ct))]);
end

```

% ALGORITMO AUXILIAR

```

function [Dr] = RandomnessImage(Im,k)
if (k == 0)
aux=reshape(Im,1,[]);
else
aux=reshape(Im',1,[]);
end
%xcorr calcula a autocorrelação normalizada (ou coeficiente de correlação cruzada)

```

do vetor aux após subtrair sua própria média .

```
AC=xcorr(aux-mean(aux),'coeff');
```

%Dr é a disentropia para $q=2$.

```
Dr=(sum((AC.^3)./(1+AC)));
```