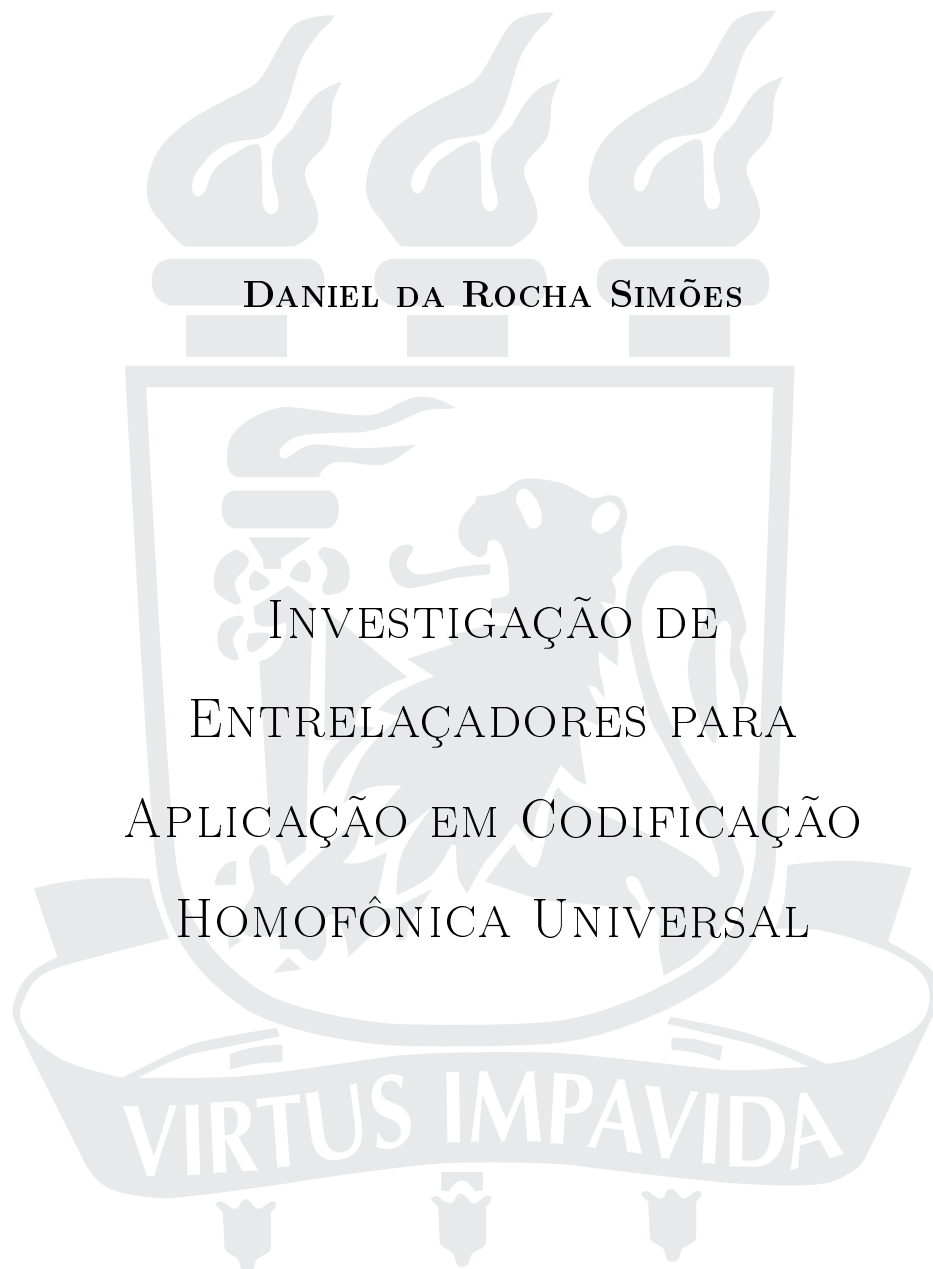


UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA



RECIFE, DEZEMBRO DE 2017.

DANIEL DA ROCHA SIMÕES

INVESTIGAÇÃO DE
ENTRELAÇADORES PARA
APLICAÇÃO EM CODIFICAÇÃO
HOMOFÔNICA UNIVERSAL

Tese submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Doutor em Engenharia Elétrica**

ORIENTADOR: PROF. VALDEMAR CARDOSO DA ROCHA JR., PH.D.

Recife, Dezembro de 2017.

©Daniel da Rocha Simões, 2017

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE TECNOLOGIA E GEOCIÊNCIAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

Daniel da Rocha Simões
**Investigação de Entrelaçadores para Aplicação
em Codificação Homofônica Universal**

‘Esta Tese foi julgada adequada para obtenção do Título de Doutor em Engenharia Elétrica, Área de Concentração em Comunicações, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco’.

Prof. Marcelo Cabral Cavalcanti, Dr.
Coordenador do Programa de
Pós-graduação em Engenharia Elétrica

Banca Examinadora:

Prof. Valdemar Cardoso da Rocha Jr., Ph.D.
Orientador
Universidade Federal de Pernambuco

Profa. Maria de Lourdes Melo Guedes Alcoforado, Dra.
Universidade de Pernambuco (UPE)

Prof. Francisco Madeiro Bernardino Jr., Dr.
Universidade de Pernambuco (UPE)

Prof. Ricardo Menezes Campello de Souza, Ph.D.
Universidade Federal de Pernambuco (UFPE)

Prof. Daniel Pedro Bezerra Chaves, Dr.
Universidade Federal de Pernambuco (UFPE)

01 de Dezembro de 2017

AGRADECIMENTOS

Agradeço, da forma mais sincera possível, às pessoas que contribuíram, direta e indiretamente, para a realização do presente trabalho.

Agradeço imensamente à minha família todo o apoio e incentivo dados durante todos os anos de minha vida acadêmica, sempre contribuindo de forma positiva à minha formação e educação. Agradeço também à minha esposa Alessandra Ouro Preto Gibson Simões a compreensão, amor e apoio diário dados da melhor forma do mundo.

Sou especialmente grato ao meu orientador, o professor Valdemar Cardoso da Rocha Jr., por ter acreditado no meu potencial e aceitado me orientar, partilhando comigo o seu conhecimento e experiência, além de ser um exemplo marcante de dedicação e profissionalismo. Muito obrigado pelo apoio dado em todas as minhas dificuldades encontradas.

Agradeço também aos professores do DES, em especial aos professores do grupo de Comunicações por todos os ensinamentos passados a mim durante esses anos de convivência, sendo também exemplos a serem seguidos, tanto no lado profissional quanto no lado pessoal.

Aos meus amigos da pós-graduação que muito colaboraram com estudos e interessantes discussões, saudável convivência, incentivos e parcerias, que dividiram comigo os momentos que passei, tornando o dia-a-dia extremamente prazeroso. Agradeço especialmente a Rodrigo Bernardino, que me apoiou bastante nos ensaios estatísticos e nos cálculos de dispersão, garantindo a disponibilidade dos computadores do laboratório da Telemática sempre que precisei.

Agradeço também os meus gestores e colegas da Andritz, que acreditaram no meu trabalho e me deram a flexibilidade necessária para que eu pudesse me dedicar às atividades do doutorado.

DANIEL DA ROCHA SIMÕES

Universidade Federal de Pernambuco

01 de Dezembro de 2017

Resumo da Tese apresentada à UFPE como parte dos requisitos necessários para a obtenção do grau de Doutor em Engenharia Elétrica

**INVESTIGAÇÃO DE ENTRELAÇADORES PARA
APLICAÇÃO EM CODIFICAÇÃO HOMOFÔNICA
UNIVERSAL**

Daniel da Rocha Simões

Dezembro/2017

Orientador: Prof. Valdemar Cardoso da Rocha Jr., Ph.D.

Área de Concentração: Comunicações

Palavras-chaves: Codificação Homofônica, Criptografia, Teoria da Informação, Entrelaçamento

Número de páginas: 153

Nesta tese, os esquemas de codificação homofônica universal *One-Time Pad – Multiplexer – Interleaver* (OMI) e *Differential Encoder – Interleaver* (DEI) são analisados, considerando o emprego do gerador de números pseudo-aleatórios de Park-Miller-Carta e de diferentes entrelaçadores paramétricos, tais como o Berrou-Glavieux, o JPL, o Co-Primo, os entrelaçadores clássicos de bloco (LRBT/LRTB/RLBT/RLTB), o Takeshita-Costello e o Welch-Costas. São apresentados cálculos parametrizados de dispersão e espalhamento de alguns desses entrelaçadores, bem como investigada a influência desses parâmetros, juntamente com o período, na qualidade estatística da sequência binária de saída dos codificadores homofônicos. Os resultados de ensaios estatísticos são apresentados considerando diferentes fontes de informação, variando-se os parâmetros do entrelaçador e a memória do codificador homofônico, mostrando que é possível realizar uma codificação homofônica eficiente com taxas elevadas, sem a necessidade do conhecimento a priori da estatística da fonte de informação. A validação desses esquemas é feita utilizando a suíte de testes estatísticos do National Institute of Standards and Technology (NIST) norte-americano, utilizando uma metodologia alternativa à que foi adotada para testar os cripto-sistemas candidatos ao Advanced Encryption Standard (AES).

Abstract of Thesis presented to UFPE as a partial fulfillment of the requirements for the degree of Doctor in Electrical Engineering

**AN INVESTIGATION OF INTERLEAVERS FOR
APPLICATION IN UNIVERSAL HOMOPHONIC
CODING**

Daniel da Rocha Simões

December/2017

Supervisor: Prof. Valdemar Cardoso da Rocha Jr., Ph.D.

Area of Concentration: Communications

Keywords: Homophonic Coding, Cryptography, Information Theory, Interleaving

Number of pages: 153

In this thesis, the One-Time Pad - Multiplexer - Interleaver (OMI) and the Differential Encoder - Interleaver (DEI) universal homophonic coding schemes are analyzed, considering the Park-Miller-Carta pseudo-number generator and different parametric interleavers (Berrou-Glavieux, JPL, Co-Prime, the classic block interleavers (LRBT/LRTB/RLBT/RLTB), Takeshita-Costello and Welch-Costas) on their implementation. The parameterized dispersion and spreading calculation of some interleavers are also presented. The influence of the interleaver period and these parameters on the statistical quality of the binary output sequence of the homophonic coders is exploited. The results of several statistical tests are presented, which consider different information sources, interleaver parameters and memory of the homophonic coders, showing that is possible to realize an efficient homophonic coding with high rates, without the previous knowledge of the information source statistics. Validation tests of the schemes are performed using the statistical test suite created by the National Institute of Standards and Technology of the United States of America, considering an alternative methodology than that used to test the Advanced Encryption Standard (AES) candidate cryptosystems.

LISTA DE FIGURAS

2.1	Cripto-sistema de chave secreta.	23
2.2	Gráfico da função equivocação de chave para cifras ideais e fortemente ideais.	25
2.3	Uso da codificação homofônica em um cripto-sistema de chave secreta.	27
2.4	Um esquema geral para a codificação homofônica.	27
2.5	Técnica de codificação homofônica clássica.	29
2.6	Técnica de codificação homofônica de comprimento variável.	29
2.7	Forma geral de codificação homofônica universal.	33
2.8	Codificador de Massey.	34
2.9	Decodificador de Massey.	34
2.10	Codificador OMI.	36
2.11	Decodificador OMI.	37
2.12	Codificador DEI.	39
2.13	Decodificador DEI.	40
3.1	Representação do produto de dois números inteiros como registradores adjacentes de 32 <i>bits</i>	48
4.1	Modelo de um entrelaçador.	50
4.2	Espalhamentos do entrelaçador LRTB de ordem 4.	53
4.3	Dispersão do entrelaçador de Berrou-Glavieux para $64 \leq T \leq 2048$	55
4.4	Dispersão do entrelaçador de Berrou-Glavieux para $4096 \leq T \leq 262144$	55
4.5	Fator λ (espalhamento) do entrelaçador de Berrou-Glavieux para $64 \leq T \leq 2048$	57
4.6	Fator λ (espalhamento) do entrelaçador de Berrou-Glavieux para $4096 \leq T \leq 262144$	57
4.7	Dispersão do entrelaçador JPL para $64 \leq T \leq 2048$	59
4.8	Dispersão do entrelaçador JPL para $4096 \leq T \leq 262144$	60

4.9	Fator λ (espalhamento) do entrelaçador JPL para $64 \leq T \leq 2048$	61
4.10	Fator λ (espalhamento) do entrelaçador JPL para $4096 \leq T \leq 262144$	61
4.11	Dispersão dos entrelaçadores clássicos de bloco para $64 \leq T \leq 2048$	64
4.12	Dispersão dos entrelaçadores clássicos de bloco para $4096 \leq T \leq 262144$	64
4.13	Fator λ (espalhamento) dos entrelaçadores LRBT e RLTB para $64 \leq T \leq 2048$	65
4.14	Fator λ (espalhamento) dos entrelaçadores LRBT e RLTB para $4096 \leq T \leq 262144$	66
4.15	Dispersão do entrelaçador Co-Primo para $64 \leq T \leq 262144$	67
4.16	Parâmetro s do entrelaçador Co-Primo quando $T = 256$	68
4.17	Dispersão do entrelaçador de Takeshita-Costello para $64 \leq T \leq 262144$	70
4.18	Fator λ (espalhamento) do entrelaçador de Takeshita-Costello para $64 \leq T \leq 262144$	71
4.19	Fator λ (espalhamento) do entrelaçador de Welch-Costas para $60 \leq T \leq 262146$	72
6.1	Resultados dos testes estatísticos para a semente $x_{01} = 12345$	84
6.2	Resultados dos testes estatísticos para a semente $x_{02} = 54321$	84
6.3	Resultados dos testes estatísticos para a semente $x_{03} = 112358$	84
6.4	Resultados dos testes estatísticos para a semente $x_{04} = 19872008$	84
6.5	Resultados dos testes estatísticos para a semente $x_{05} = 26011982$	84
6.6	Codificador OMI/DEI com $n = 1$	85
6.7	Imagem da fonte “Cana 51”.	86
6.8	Imagem da fonte “Platão”.	86
6.9	Imagem da fonte “SC06”.	86
6.10	Resultados do Ensaio 1 envolvendo o entrelaçador BGL.	92
6.11	Resultados do Ensaio 1 envolvendo o entrelaçador JPL.	93
6.12	Resultados do Ensaio 1 envolvendo o entrelaçador LRTB.	94
6.13	Resultados do Ensaio 1 envolvendo o entrelaçador CPR.	95
6.14	Resultados do Ensaio 1 envolvendo o entrelaçador TKC.	95
6.15	Resultados do Ensaio 1 envolvendo o entrelaçador WLC.	96
6.16	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI.	101
6.17	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI.	102

6.18	Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI.	104
6.19	Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador DEI.	105
6.20	Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI.	106
6.21	Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI.	107
B.1	Resultados do Ensaio 1 envolvendo o entrelaçador BGL.	123
B.2	Resultados do Ensaio 1 envolvendo o entrelaçador JPL.	124
B.3	Resultados do Ensaio 1 envolvendo o entrelaçador LRTB.	125
B.4	Resultados do Ensaio 1 envolvendo o entrelaçador CPR.	126
B.5	Resultados do Ensaio 1 envolvendo o entrelaçador TKC.	127
B.6	Resultados do Ensaio 1 envolvendo o entrelaçador WLC.	128
B.7	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Agatha”.	130
B.8	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Agatha”.	131
B.9	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Cana51”.	132
B.10	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Cana51”.	133
B.11	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Platão”.	134
B.12	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Platão”.	135
B.13	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “SC06”.	136
B.14	Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “SC06”.	137
B.15	Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI processando a fonte “Agatha”.	138

B.16 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador DEI processando a fonte “Agatha”.	139
B.17 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI processando a fonte “Cana51”.	140
B.18 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador DEI processando a fonte “Cana51”.	141
B.19 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI processando a fonte “Platão”.	142
B.20 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador DEI processando a fonte “Platão”.	143
B.21 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI processando a fonte “SC06”.	144
B.22 Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador DEI processando a fonte “SC06”.	145
B.23 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI processando a fonte “Agatha”.	146
B.24 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI processando a fonte “Agatha”.	147
B.25 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI processando a fonte “Cana51”.	148
B.26 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI processando a fonte “Cana51”.	149
B.27 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI processando a fonte “Platão”.	150
B.28 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI processando a fonte “Platão”.	151
B.29 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI processando a fonte “SC06”.	152
B.30 Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI processando a fonte “SC06”.	153

LISTA DE TABELAS

4.1	Números primos definidos para o entrelaçador de Berrou-Glavieux.	54
4.2	Expressões analíticas para a dispersão e para a dispersão normalizada do entrelaçador de Berrou-Glavieux.	56
4.3	Números primos definidos para o entrelaçador JPL.	59
4.4	Parâmetros considerados para o entrelaçador Co-Primo.	67
4.5	Pontos máximos e mínimos da curva do parâmetro s do entrelaçador Co-Primo.	69
4.6	Parâmetros considerados para o entrelaçador de Takeshita-Costello.	69
4.7	Parâmetros considerados para o entrelaçador de Welch-Costas.	72
5.1	Conclusões de um teste estatístico.	74
5.2	Descrição geral de cada um dos testes da suíte do NIST.	76
5.3	Valores recomendados para os parâmetros de entrada dos testes estatísticos do NIST.	77
5.4	Parâmetros padrão da suíte de testes do NIST.	77
5.5	Limite de confiança para $k = 100$ sequências testadas.	80
5.6	Informações parciais contidas no arquivo “finalAnalysisReport”.	81
5.7	Probabilidades em percentual de uma sequência falhar em i testes estatísticos.	82
6.1	Fontes consideradas para a realização dos ensaios estatísticos.	85
6.2	Períodos e parâmetros considerados para os entrelaçadores BGL, JPL e LRTB.	88
6.3	Períodos e parâmetros considerados para os entrelaçadores CPR e TKC (parte 1).	89
6.4	Períodos e parâmetros considerados para os entrelaçadores CPR e TKC (parte 2).	90
6.5	Períodos e parâmetros considerados para o entrelaçador WLC.	91

6.6	Dispersões normalizadas dos entrelaçadores BGL e JPL para $T_1 = 131072$ e $T_2 = 262144$	98
6.7	Parâmetros associados aos casos de sucesso no Ensaio 1.	100
6.8	Taxas atingidas e período requerido (entrelaçador) para os esquemas de codificação homofônica universal OMI e DEI.	108
B.1	Figuras associadas aos testes estatísticos do Ensaio 1, envolvendo as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.	122
B.2	Figuras associadas aos testes estatísticos do Ensaio 2, envolvendo as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.	129

LISTA DE ABREVIATURAS

AES	<i>Advanced Encryption Standard</i>
BGL	Entrelaçador de Berrou-Glavieux
CCSDS	Comitê Consultivo para Sistemas Espaciais de Dados (<i>Consultative Committee for Space Data Systems</i>)
CPR	Entrelaçador Co-Primo
DEI	Codificador Diferencial - Entrelaçador (<i>Differential Encoder - Interleaver</i>)
DES	<i>Data Encryption Standard</i>
DSES	Fonte Discreta Estacionária e Ergódica (<i>Discrete Stationary Ergodic Source</i>)
IID	Independente e Identicamente Distribuído
JKM	Código homofônico de Jendal-Kuhn-Massey
JPL	Laboratório de Propulsão a Jato (<i>Jet Propulsion Laboratory</i>)
KS	Teste estatístico de Kolmogorov-Smirnov
LFSR	Registrador de Deslocamento com Realimentação Linear (<i>Linear Feedback Shift Register</i>)
LRBT	Esquerda-Direita Baixo-Cima (<i>Left-Right Bottom-Top</i>)
LRTB	Esquerda-Direita Cima-Baixo (<i>Left-Right Top-Bottom</i>)
LZW	Código de fonte de Lempel-Ziv-Welch
NASA	Agência Espacial Americana (<i>National Aeronautics and Space Administration</i>)
NIST	Instituto Nacional de Padrões e Tecnologia (<i>National Institute of Standards and Technology</i>)
OMI	Cifra de Blocos Descartáveis - Multiplexador - Entrelaçador (<i>One-Time Pad - Multiplexer - Interleaver</i>)
PMC	Gerador de Números Pseudo-Aleatórios de Park-Miller-Carta
PRNG	Gerador de Números Pseudo-Aleatórios (<i>Pseudo-Random Number Generator</i>)
RLBT	Direita-Esquerda Baixo-Cima (<i>Right-Left Bottom-Top</i>)
RLTB	Direita-Esquerda Cima-Baixo (<i>Right-Left Top-Bottom</i>)
RM	Código homofônico de Rocha-Massey

RNG	Gerador de Números Aleatórios (<i>Random Number Generator</i>)
RSA	Cifra de Rivest-Shamir-Adleman
SIPI	<i>Signal and Image Processing Institute</i>
TKC	Entrelaçador de Takeshita-Costello
USC	<i>University of Southern California</i>
WLC	Entrelaçador de Welch-Costas

SUMÁRIO

1	INTRODUÇÃO	17
1.1	Motivação	17
1.2	Objetivos e Contribuições	19
1.3	Estrutura da Tese	20
2	CODIFICAÇÃO HOMOFÔNICA	22
2.1	Introdução	22
2.2	Criando Cifras Fortemente Ideais	23
2.3	Conceitos de Codificação Homofônica	26
2.3.1	Codificação Homofônica Clássica	28
2.3.2	Codificação Homofônica de Comprimento Variável	28
2.3.3	Parâmetros de Desempenho de um Codificador Homofônico	29
2.4	Codificação Homofônica Universal	33
2.4.1	O Codificador de Massey	34
2.4.2	O Codificador OMI	36
2.4.3	O Codificador DEI	39
3	GERAÇÃO DE NÚMEROS PSEUDO-ALEATÓRIOS	41
3.1	Introdução	41
3.2	Geradores de Números Aleatórios (RNGs)	42
3.3	Geradores de Números Pseudo-Aleatórios (PRNGs)	44
3.4	O gerador Congruencial Linear de Park-Miller	46
3.4.1	Descrição do Gerador	46
3.5	Otimizações na Implementação do Gerador	48

4	FUNDAMENTOS DE ENTRELAÇADORES	50
4.1	Introdução	50
4.2	A Dispersão de um Entrelaçador	51
4.3	O Espalhamento de um Entrelaçador	52
4.4	Alguns Entrelaçadores Paramétricos	53
4.4.1	O Entrelaçador de Berrou-Glavieux (BGL)	54
4.4.2	O Entrelaçador JPL	58
4.4.3	Os Entrelaçadores Clássicos de Bloco	62
4.4.4	O Entrelaçador Co-Primo (CPR)	67
4.4.5	O Entrelaçador de Takeshita-Costello (TKC)	69
4.4.6	O Entrelaçador de Welch-Costas	71
5	AVALIAÇÕES DE ALEATORIEDADE	73
5.1	Introdução	73
5.2	A Suíte de Testes Estatísticos do NIST	75
5.2.1	Interpretação dos Resultados	78
6	ANÁLISE DOS ENSAIOS ESTATÍSTICOS	83
6.1	Análise do Gerador de Números Pseudo-Aleatórios	83
6.2	Análise do Codificador OMI/DEI com $n = 1$ (Ensaio 1)	85
6.2.1	Fontes de Informação	85
6.2.2	Objetivo e Metodologia do Ensaio 1	87
6.2.3	Resultados Envolvendo o Entrelaçador BGL	92
6.2.4	Resultados Envolvendo o Entrelaçador JPL	93
6.2.5	Resultados Envolvendo o Entrelaçador LRTB	94
6.2.6	Resultados Envolvendo o Entrelaçador CPR	94
6.2.7	Resultados Envolvendo o Entrelaçador TKC	95
6.2.8	Resultados Envolvendo o Entrelaçador WLC	96
6.2.9	Comentários para o Ensaio 1	97
6.3	Análise do Codificador OMI/DEI com $n > 1$ (Ensaio 2)	99
6.3.1	Objetivo e Metodologia do Ensaio 2	100
6.3.2	Resultados Envolvendo o Entrelaçador BGL	100
6.3.3	Resultados Envolvendo o Entrelaçador TKC	103

6.3.4	Resultados Envolvendo o Entrelaçador WLC	106
6.3.5	Comentários para o Ensaio 2	108
7	CONCLUSÕES	109
7.1	Sugestões para Trabalhos Futuros	110
Apêndice A	GERADOR DE PARK-MILLER-CARTA - ABORDAGEM TEÓRICA	116
Apêndice B	OUTROS RESULTADOS DOS ENSAIOS ESTATÍSTICOS	122
B.1	Ensaio 1	122
B.2	Ensaio 2	129

CAPÍTULO 1

INTRODUÇÃO

1.1 Motivação

A criptografia é uma ferramenta que tem como objetivo garantir o sigilo, a integridade e a autenticidade de dados e entidades, e inicialmente foi utilizada somente para fins militares e diplomáticos. Durante a Segunda Guerra Mundial, houve um grande desenvolvimento na área, sendo criadas novas técnicas e também sendo construídas máquinas para cifrar e decifrar, como a máquina alemã ENIGMA [1]. Devido ao desenvolvimento dos meios de comunicação, as técnicas de criptografia passaram a ser mais acessíveis, sendo disseminadas a várias áreas e encontrando diversas aplicações. Paralelamente ao avanço de técnicas de cifragem, desenvolveram-se também os métodos de criptoanálise, resultando na quebra de diversos cripto-sistemas.

Na prática, os dados a serem protegidos por meio da criptografia possuem, em geral, um comportamento estatístico muito diferente daquele apresentado por dados produzidos por uma fonte aleatória, ou seja, por uma fonte que produz símbolos estatisticamente independentes e uniformemente distribuídos. Tal comportamento representa uma vulnerabilidade que, caso não tratada adequadamente, certamente pode ser explorada por terceiros. Assim, essa excessiva redundância do texto claro motivou o aparecimento da codificação homofônica, que é uma técnica utilizada na criptografia para combater ataques que exploram desvios na estatística do texto cifrado como, por exemplo, a análise da frequência relativa dos símbolos. Tais sistemas são interessantes para aplicação prática, contribuindo para tornar os cripto-sistemas de chave secreta, conhecidos também como cripto-sistemas simétricos, mais resistentes à criptoanálise.

Isto faz com que um usuário não autorizado, analisando o texto cifrado, não consiga obter informações sobre a chave utilizada na cifra nem sobre o texto claro, ataque conhecido como *ciphertext-only-attack*.

Embora não se saiba quem percebeu em primeiro lugar que as frequências das letras podiam ser exploradas de modo a quebrar cifras, a mais antiga descrição conhecida dessa técnica vem de um cientista do século IX, Abu Yusef Ya'qub ibn Is-haq ibn as-Sabbah ibn omran ibn Ismail al-Kindi. Conhecido como “o filósofo dos árabes”, al-Kindi foi o autor de um tratado que só foi redescoberto em 1987, no Arquivo Otomano Sulaimaniyyah em Istambul, intitulada “Um manuscrito sobre a decifração de mensagens criptográficas”. No século XV, esse conhecimento sobre a análise de frequência de ocorrência das letras de uma mensagem foi utilizado por Simeone de Crema, em 1401, e Michele Steno de Veneza, de 1400 a 1413. Nas cifras de Simeone, utilizava-se uma chave na qual cada vogal do texto original possuía vários equivalentes, enquanto que nas cifras de Michele, escolhia-se um dos muitos símbolos para cada caracter, além de utilizar caracteres mudos e outros caracteres especiais para certas palavras de uso frequente. Em 1595, Henrique IV, rei da França e Navarra, utilizava uma cifra homofônica particular para os assuntos sigilosos. Um pouco mais elaborada, além das vogais havia outras letras frequentes com mais de um substituto. Em 1628, Luis XIII usava uma cifra homofônica própria. Na mesma época, a correspondência de assuntos estrangeiros entre Constantinopla e a França também era cifrada e possuía um método próprio [2].

A codificação homofônica consiste na substituição de cada símbolo da mensagem original por um ou mais símbolos, pertencentes a um alfabeto maior, de forma a produzir símbolos estatisticamente independentes e uniformemente distribuídos. Essa técnica reduz a redundância da mensagem a ser cifrada tendo como custo uma expansão do texto claro. Esses símbolos são denominados homofonemas, palavra que deriva do grego e significa “do mesmo som”. O número de homofonemas destinados a representar a cada símbolo da mensagem deve ser proporcional à sua frequência de ocorrência no texto claro. Em textos na língua portuguesa, por exemplo, as letras A, E e O (de alta frequência) teriam vários substitutos possíveis enquanto que J, X e Z teriam apenas um.

Na sua forma clássica, esse procedimento necessita do conhecimento prévio da estatística do texto claro para realizar a codificação. Apesar desta técnica ser conhecida há muitos anos, foi apenas em 1988 que Günther descreveu um algoritmo para a realização de codificação homofônica, no qual as palavras representando homofonemas podem ter comprimento variável

[3]. Esse algoritmo é detalhado sob o ponto de vista da teoria da informação em [4]. Em [5, 6], é apresentado um esquema de codificação homofônica perfeita, em que as palavras-código são completamente aleatórias. Na maioria das aplicações práticas, em geral, não se tem *a priori* o conhecimento da estatística da fonte, de modo que procedimentos de codificação homofônica para fontes específicas tornam-se bastante ineficientes nessa situação. Surge então a necessidade de se desenvolver sistemas que realizam a codificação de forma universal, ou seja, não precisam do conhecimento *a priori* da estatística da fonte para realizar a codificação.

J. Massey foi o primeiro a propor um esquema de codificação homofônica universal, em 1994. Sua abordagem emprega um multiplexador e um codificador universal de fonte [7]. Apesar de a sequência de saída do codificador de Massey apresentar uma alta entropia, ela possui diversos desvios estatísticos, que serviu de motivação para o surgimento de novos esquemas. Em 2009, foram propostos os codificadores homofônicos universais denominados *One-Time Pad - Multiplexer - Interleaver* (OMI) [8, 9] e *Differential Encoder - Interleaver* (DEI) [10, 11], se tornando alternativas de simples implementação e mais eficientes do que o esquema proposto por Massey.

1.2 Objetivos e Contribuições

Em [8–10], as sequências de saída dos codificadores homofônicos universais OMI e DEI são analisadas utilizando a suíte de testes estatísticos do *National Institute of Standards and Technology* norte-americano (NIST) [12], considerando a aplicação do entrelaçador de Berrou-Glavieux [13, 14]. Neste trabalho, é realizada uma análise de desempenho desses codificadores homofônicos considerando o emprego do gerador de número pseudo-aleatórios de Park-Miller-Carta e a aplicação de outros entrelaçadores determinísticos, como o JPL [15], os entrelaçadores clássicos de bloco (LRBT, LRTB, RLBT e RLTB), o Co-Primo, o entrelaçador de Takeshita-Costello [16] e o entrelaçador de Welch-Costas [17]. Essa análise é realizada utilizando uma versão otimizada da suíte de testes do *National Institute of Standards and Technology* (NIST) [18], adotando uma metodologia alternativa à que foi adotada para testar os cripto-sistemas candidatos ao Advanced Encryption Standard (AES).

O objetivo é investigar se existe influência dos parâmetros de dispersão, espalhamento ou parâmetros próprios desses entrelaçadores na qualidade estatística das sequências de saída dos esquemas propostos de codificação homofônica universal. São apresentadas também análises e expressões analíticas para o cálculo dos parâmetros de dispersão e espalhamento de alguns

entrelaçadores. Essas informações permitem definir as diretrizes para o projeto de entrelaçadores customizados para maximizar a eficiência dos codificadores homofônicos propostos e contribuir para tornar os cripto-sistemas não expansivos mais resistentes contra ataques que exploram desvios estatísticos no texto cifrado.

1.3 Estrutura da Tese

Este trabalho está organizado em sete capítulos. O Capítulo 2 apresenta alguns fundamentos da codificação homofônica. A Seção 2.1 apresenta uma breve introdução ao tema, enquanto que a Seção 2.2 ilustra a motivação e o contexto da utilização da codificação homofônica na criptografia. A Seção 2.3 apresenta alguns fundamentos de codificação homofônica clássica e da codificação homofônica de comprimento variável introduzida por C. Günther [3]. Também são apresentados os parâmetros de desempenho de um codificador homofônico. A Seção 2.4 trata dos fundamentos da codificação homofônica universal, apresentando o esquema proposto por J. L. Massey [7], o codificador OMI e o codificador DEI.

O Capítulo 3 trata da geração de números pseudo-aleatórios. Nesse capítulo, além de uma breve introdução (Seção 4.1), abordam-se alguns conceitos dos geradores de números aleatórios (RNGs) e dos geradores de números pseudo-aleatórios (PRNGs) (Seções 3.2 e 3.3). O gerador congruencial linear de Park-Miller-Carta [19, 20] é descrito na Seção 3.4 e as otimizações em sua implementação são discutidas na Seção 3.5.

O Capítulo 4 trata de alguns fundamentos de entrelaçadores. A Seção ?? apresenta algumas definições relativas ao entrelaçador. As Seções 4.2 e 4.3 apresentam as definições da dispersão e do espalhamento de um entrelaçador, respectivamente. Finalmente, a Seção 4.4 apresenta as descrições e a análise dos entrelaçadores de Berrou-Glavieux (versão corrigida em relação ao livro de C. Heegard [21]), JPL, dos entrelaçadores clássicos de bloco, Co-Primo, de Takeshita-Costello e de Welch-Costas.

O Capítulo 5 trata de avaliações de aleatoriedade em uma sequência binária. A Seção 5.1 apresenta algumas premissas, hipóteses e métricas utilizadas por um teste estatístico na avaliação da aleatoriedade de uma sequência. A Seção 5.2 trata da suíte de testes estatísticos do NIST, apresentando uma descrição geral de cada um dos testes, os parâmetros recomendados e também apresentando a metodologia adotada neste trabalho para a interpretação dos resultados.

O Capítulo 6 trata da análise e resultados envolvendo simulações em computador dos

esquemas de codificação homofônica universal discutidos na Seção 2.4. A Seção 6.1 trata da análise do gerador de números pseudo-aleatórios de Park-Miller-Carta, apresentado no Capítulo 3. Na Seção 6.2, é apresentada a análise do codificador OMI/DEI com $n = 1$ mostrando a metodologia adotada e os resultados associados à fonte de informação de referência, variando os entrelaçadores, considerando períodos e parâmetros diferentes. Na Seção 6.3, é apresentada a análise e as conclusões dos ensaios envolvendo os codificadores OMI e DEI com $n > 1$, mostrando as taxas nos quais esses esquemas conseguem atingir.

O Capítulo 7 apresenta as conclusões deste trabalho e também as sugestões para trabalhos futuros. A tese ainda conta com dois apêndices: o Apêndice A, que contém a teoria envolvida na concepção do gerador de números pseudo-aleatórios de Park-Miller-Carta e o Apêndice B, que apresenta os resultados dos ensaios estatísticos realizados nas Seções 6.2 e 6.3, considerando as demais fontes de informação adotadas neste trabalho.

CAPÍTULO 2

CODIFICAÇÃO HOMOFÔNICA

2.1 Introdução

A codificação homofônica é uma técnica utilizada para converter uma sequência de texto claro em uma sequência mais aleatória. Essa técnica consiste na substituição de cada símbolo da mensagem original por um ou mais símbolos, denominados homofonemas (palavra de origem grega, significando “do mesmo som”), pertencentes a um alfabeto maior, de forma a produzir símbolos uniformemente distribuídos e estatisticamente independentes, reduzindo assim a redundância da mensagem. Esse procedimento torna os cripto-sistemas não-expansíveis de chave secreta mais seguros pois ele aumenta a distância de unicidade da cifra. Em um trabalho pioneiro, Günther descreveu um algoritmo para a realização desse tipo de codificação homofônica, em que as palavras representando homofonemas podem ter comprimento variável [3].

Na maioria das aplicações práticas, não se tem *a priori* o conhecimento da estatística da fonte, de modo que, procedimentos de codificação para fontes arbitrárias tornam-se bastante ineficientes nessa situação. Surge então a necessidade de se desenvolver sistemas que realizam a codificação de forma universal, ou seja, não precisam do conhecimento *a priori* da estatística da fonte para realizar a codificação.

2.2 Criando Cifras Fortemente Ideais

Considere o cripto-sistema de chave secreta ilustrado pela Figura 2.1. Sejam o texto claro $[X_1, X_2, \dots, X_n]$, denotado por X^n , e o texto cifrado $[Y_1, Y_2, \dots, Y_n]$, denotado por Y^n , e a chave secreta Z , que assume-se estatisticamente independente do texto claro X^n , para qualquer valor de n inteiro.

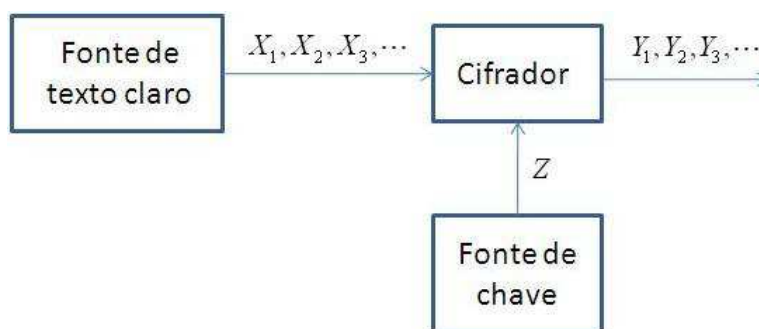


Figura 2.1: Cripto-sistema de chave secreta.

Definição 2.1 (Cifra não-expansiva) *Define-se uma cifra não-expansiva como uma cifra em que o texto claro e o texto cifrado possuem o mesmo alfabeto e existe uma sequência infinita de inteiros positivos n_1, n_2, n_3, \dots tal que os primeiros n_i símbolos Y_1, Y_2, \dots, Y_{n_i} do texto cifrado junto com a chave secreta determinam unicamente os primeiros n_i símbolos X_1, X_2, \dots, X_{n_i} do texto claro para $i = 1, 2, 3, \dots$.*

Como exemplo de cifra não-expansiva pode ser citada a cifra de fluxo aditiva, em que $Y_i = X_i \oplus Z'_i$. A sequência Z'_1, Z'_2, Z'_3, \dots é uma chave de seção gerada a partir da chave secreta Z . Outro exemplo é a cifra de bloco, em que os blocos de texto claro e de texto cifrado possuem o mesmo comprimento N . Para o caso da cifra de fluxo aditiva, tem-se $n_i = i$ e para o caso da cifra de bloco, tem-se $n_i = iN$.

Uma sequência D -ária é dita completamente aleatória se cada um dos seus dígitos é estatisticamente independente dos dígitos precedentes e a escolha dos D valores possíveis é equiprovável. A propriedade conhecida como *random-in/random-out*, definida a seguir, vale para as cifras não-expansivas [7]:

Proposição 2.1 *Se uma sequência de texto claro X^n , cifrada por uma cifra de chave secreta não-expansível, for completamente aleatória, então a sequência de texto cifrado Y^n também é completamente aleatória, para qualquer escolha z da chave Z . Além disso, Y^n é esta-*

tisticamente independente da chave secreta Z para qualquer que seja a sua distribuição de probabilidade.

Demonstração: Partindo da regra da cadeia para a incerteza, dada por

$$H(X_1, X_2, \dots, X_N) = H(X_1) + H(X_2|X_1) + \dots + H(X_N|X_1 \dots X_{N-1}),$$

tem-se

$$\begin{aligned} H(X^n, Y^n, Z) &= H(X^n) + H(Z|X^n) + H(Y^n|X^n, Z) \\ &= H(Y^n) + H(Z|Y^n) + H(X^n|Y^n, Z). \end{aligned}$$

Sabendo que $H(Y^n|X^n, Z) = H(X^n|Y^n, Z) = 0$, tem-se

$$H(Y^n) = H(X^n) + H(Z|X^n) - H(Z|Y^n).$$

Mas, como assumiu-se que X^n e Z são estatisticamente independentes, então $H(Z|X^n) = H(Z)$. Além disso, uma vez que X^n é completamente aleatória, então $H(X^n) = n \log D$. Logo,

$$H(Y^n) = n \log D + H(Z) - H(Z|Y^n) \geq n \log D.$$

Por outro lado, utilizando a desigualdade fundamental da Teoria da Informação $\log r \leq (r - 1) \log e, \forall r$ real, chega-se a $H(Y^n) \leq n \log D$, com igualdade se e somente se Y^n for completamente aleatória.

Assim, tem-se que $H(Y^n) = n \log D = H(X^n)$ e $H(Z|Y^n) = H(Z)$, implicando que Y^n é completamente aleatória e independente de Z . ■

Shannon definiu a função equivocação de chave de uma cifra de chave secreta como sendo a entropia condicional da chave dados os n primeiros dígitos do texto cifrado, ou seja, $f(n) = H(Z|Y^n)$ [22]. Como $f(n)$ decresce à medida que n cresce, Shannon deu as seguintes denominações a um cripto-sistema:

Ideal Se $f(n)$ se aproxima de um valor positivo quando n tende ao infinito,

$$\lim_{n \rightarrow \infty} f(n) = A, \quad A > 0; \quad (2.1)$$

Fortemente ideal Se a sequência de texto cifrado for estatisticamente independente da chave, ou seja, $f(n)$ é constante e igual a $H(Z)$,

$$f(n) = H(Z|Y^n) = H(Z). \quad (2.2)$$

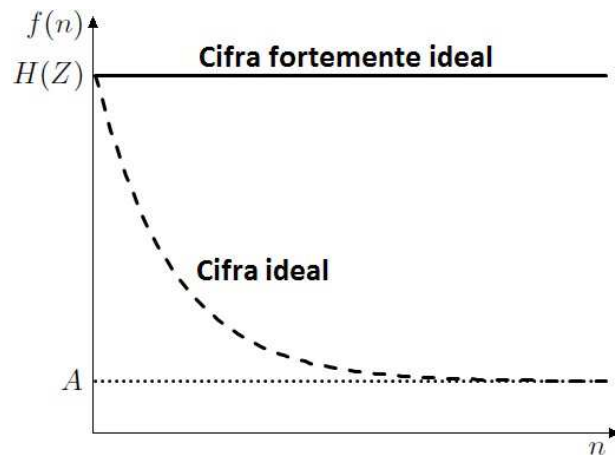


Figura 2.2: Gráfico da função equivocação de chave para cifras ideais e fortemente ideais.

A Figura 2.2 ilustra essas duas denominações no gráfico de $f(n)$.

Corolário 2.1 *Se uma sequência de texto claro X^n , cifrada por uma cifra de chave secreta não-expansível, for completamente aleatória, então o cripto-sistema é dito fortemente ideal, independentemente da distribuição de probabilidade da chave secreta Z [4].*

O Corolário 2.1 implica que em um ataque ao texto cifrado, não se pode obter nenhuma informação sobre a chave secreta Z , não importando a quantidade.

Definição 2.2 (Cifra não-degenerativa) *Uma cifra não-degenerativa é aquela em que mudando o valor de Z , sem mudar o valor da sequência de texto claro X^n , o valor da sequência de texto cifrado Y^n mudará para todo n suficientemente grande. Equivalentemente, uma cifra é não-degenerativa se, quando todos os valores da chave Z são equiprováveis, tem-se*

$$H(Y^n|X^n) \approx H(Z), \quad (2.3)$$

para todo n suficientemente grande e todas as distribuições de probabilidade de X^n .

Proposição 2.2 *Nas cifras não-expansivas, tem-se que*

$$H(X^n|Y^n) = H(Y^n|X^n) \quad (2.4)$$

quando a sequência X^n de texto claro é completamente aleatória [4].

Demonstração: Partindo da regra da cadeia para a incerteza, tem-se

$$\begin{aligned} H(X^n, Y^n) &= H(X^n) + H(Y^n|X^n) \\ &= H(Y^n) + H(X^n|Y^n). \end{aligned}$$

Como X^n é completamente aleatória, então Y^n também o é (Proposição 2.1), o que leva a $H(X^n) = H(Y^n) = n \log D$. Logo, tem-se $H(X^n|Y^n) = H(Y^n|X^n)$. ■

Corolário 2.2 *Se uma sequência de texto claro X^n cifrada por uma cifra de chave secreta não-expansível for completamente aleatória e todos os possíveis valores da chave secreta Z forem equiprováveis, então a entropia condicional do texto claro dado o texto cifrado satisfaz*

$$H(X^n|Y^n) \approx H(Z), \quad (2.5)$$

para todo n suficientemente grande [4].

Assim, num ataque ao texto cifrado, a dificuldade de um criptoanalista determinar X^n é a mesma de adivinhar qual a chave Z utilizada dentre as muitas possibilidades de escolha, o que torna esse tipo de ataque inviável.

Como foi mostrado, dado que a fonte de texto claro emite uma sequência completamente aleatória, qualquer cifra de chave secreta não-expansiva pode se tornar fortemente ideal. O objetivo da codificação homofônica é justamente transformar uma fonte não-aleatória em uma fonte que emite sequências completamente aleatórias. Essa técnica pode ser encarada como um pré-processamento do texto claro para tornar uma determinada cifra de chave secreta fortemente ideal, fortalecendo-a contra ataques que exploram desvios estatísticos no texto cifrado.

2.3 Conceitos de Codificação Homofônica

A Figura 2.3 ilustra o uso de um codificador homofônico em um cripto-sistema de chave secreta. O texto claro é o resultado da codificação da sequência de símbolos L -ários ($2 \leq L < \infty$) denotados por U_1, U_2, \dots , que sai da fonte de mensagem, em uma sequência de símbolos D -ários denotados por X_1, X_2, \dots .

Para tornar a análise mais simples, assume-se que a fonte de mensagem é sem memória e estacionária, ou seja, que U_1, U_2, \dots é uma sequência L -ária independente e identicamente distribuída (IID), reduzindo assim o problema de codificação da fonte de mensagem a um problema de codificação de uma única variável aleatória, diga-se $U = U_1$. Assume-se também que todos os L valores de U possuem probabilidade não-nula.

Quando $L = D^W$ para algum W inteiro e positivo e quando todos os L valores possíveis de U são equiprováveis, uma técnica simples de codificação relaciona cada uma das D^W

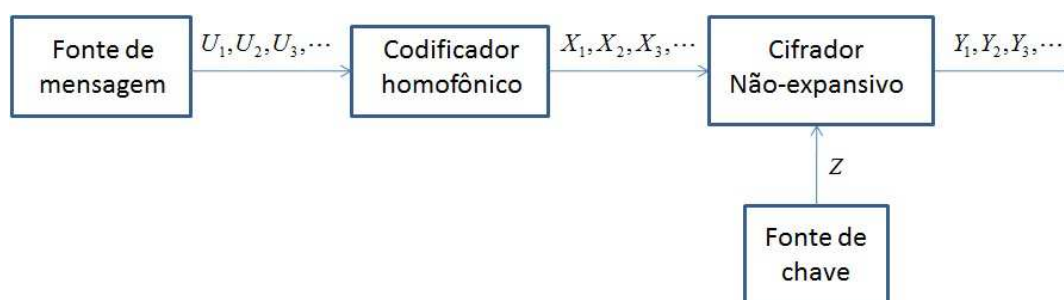


Figura 2.3: Uso da codificação homofônica em um cripto-sistema de chave secreta.

sequências D -árias de comprimento W a cada valor de U , o que faz com que a palavra-código $X_1, X_2, X_3, \dots, X_W$ seja completamente aleatória.

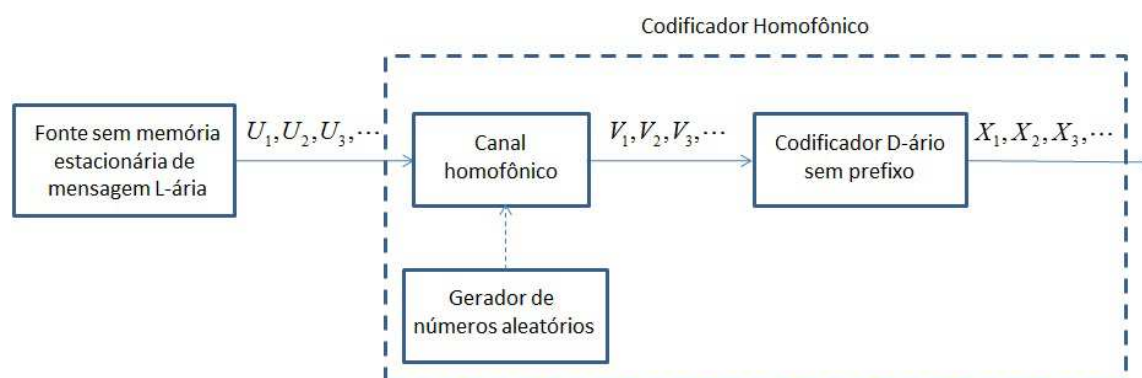


Figura 2.4: Um esquema geral para a codificação homofônica.

A Figura 2.4 ilustra o esquema geral para a codificação homofônica. O canal homofônico é um canal sem memória cujo alfabeto de entrada $\{u_1, u_2, \dots, u_L\}$ coincide com o conjunto de possíveis valores de U , o alfabeto de saída $\{v_1, v_2, v_3, \dots\}$ pode ser finito ou infinito contável, e as probabilidades de transição $P(V = v_j | U = u_i)$ possuem a propriedade de que, para cada j , existe exatamente um i tal que $P(V = v_j | U = u_i) \neq 0$. Considera-se que os v_j , em que $P(V = v_j | U = u_i) > 0$, são os homofonemas de u_i . O canal homofônico é um canal sem ruído, ou seja, é um canal em que existem pelo menos tantos símbolos de saída quanto símbolos de entrada, em que cada símbolo de saída pode ser produzido pela ocorrência de apenas um dos símbolos de entrada. O codificador D -ário é um dispositivo que associa uma sequência D -ária a cada v_j , de modo que a palavra-código associada seja distinta das outras palavras-código e também não seja prefixo de outra palavra-código mais longa, o que garante que em uma sequência X_1, X_2, \dots de palavras-código, o fim de cada palavra-código possa ser identificado imediatamente sem que seja necessária a verificação de nenhum símbolo seguinte na sequência. O canal homofônico junto com o codificador D -ário é referido como codificador

homofônico. Supõe-se que um gerador de números aleatórios externo provê os *bits* necessários para a escolha dos homofonemas. A Figura 2.4 pode descrever as seguintes situações:

Codificação de fonte usual: Quando o canal homofônico é determinístico, ou seja, quando todas as probabilidades de transição não-nulas são iguais a 1 ($V = U$).

Codificação homofônica clássica: Quando o canal homofônico é não-trivial, mas a codificação binária é trivialmente livre de prefixo, porque todas as palavras-código possuem o mesmo comprimento, ou seja, o código é um código de bloco.

Codificação homofônica de comprimento variável: Quando o canal homofônico é determinístico e a codificação livre de prefixo é não-trivial.

Apesar da simplicidade do esquema ilustrado, sua principal desvantagem é que ele não é facilmente adaptável à mudança da estatística da fonte [7].

2.3.1 Codificação Homofônica Clássica

Quando os valores de U não são equiprováveis, a *codificação homofônica clássica* escolhe, se possível, um valor de W apropriado com $D^W > L$, particionando as D^W sequências D -árias de comprimento W em L subconjuntos, relacionando a cada um desses subconjuntos um valor de U de modo que o número de sequências em cada subconjunto seja proporcional à probabilidade do correspondente valor de U . Assim, a palavra-código para um valor particular u de U é obtida por uma escolha equiprovável do subconjunto de sequências (homofonemas) correspondentes a u , cuja distribuição de probabilidade segue uma distribuição uniforme. Quando tal partição das sequências D -árias de comprimento W é possível, a palavra-código X_1, X_2, \dots, X_W pode assumir, de forma equiprovável, quaisquer das sequências D -árias de mesmo comprimento W de modo que a sequência X_1, X_2, \dots, X_W seja completamente aleatória.

2.3.2 Codificação Homofônica de Comprimento Variável

Günther introduziu a codificação homofônica de comprimento variável, que é uma generalização da codificação homofônica clássica [3]. Nessa técnica, as sequências D -árias podem ter comprimentos diferentes e as probabilidades de seleção dos homofonemas associados a um valor particular u de U podem ser diferentes. O comprimento W da palavra-código X_1, X_2, \dots, X_W de U pode, portanto, ser uma variável aleatória. Günther idealizou um algoritmo de codificação homofônica de comprimento variável com $D = 2$ que torna a palavra-código binária

resultante X_1, X_2, \dots, X_W uma sequência completamente aleatória [3]. Quando $L = 2^n$, o algoritmo constrói uma palavra-código cujo comprimento $E(W)$ pode ser menor do que n , de modo que o algoritmo também realiza uma compressão de dados.

A Figura 2.5 ilustra um exemplo da técnica de codificação homofônica clássica para uma fonte de mensagem binária ($L = 2$), com probabilidades $P(U = u_1 = \frac{1}{4})$ e $P(U = u_2 = \frac{3}{4})$.

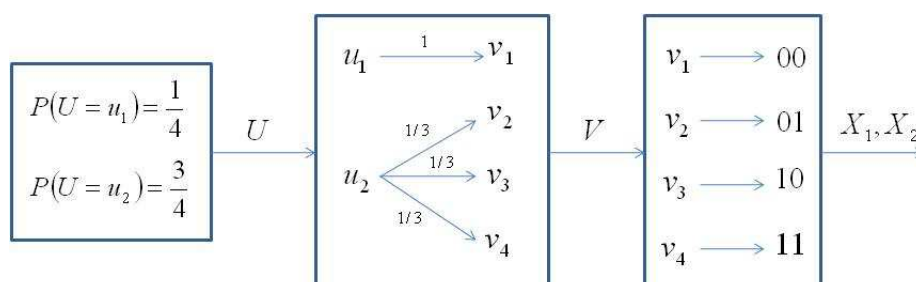


Figura 2.5: Técnica de codificação homofônica clássica.

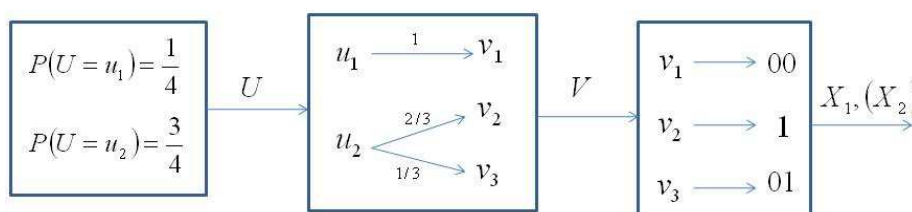


Figura 2.6: Técnica de codificação homofônica de comprimento variável.

A Figura 2.6 ilustra um exemplo da técnica de codificação homofônica de comprimento variável para a mesma fonte da Figura 2.5, utilizando um codificador de Huffman na saída do canal homofônico. Quando a fonte de mensagem produz o símbolo u_1 , o canal homofônico tem como saída a palavra-código v_1 , e a palavra-código gerada pelo código de Huffman é $x_1 = 00$. Se a fonte produzir o símbolo u_2 , sua representação será tanto v_2 ou v_3 , escolhido aleatoriamente: v_2 é escolhido com probabilidade $\frac{2}{3}$, e v_3 com probabilidade $\frac{1}{3}$. Nota-se que o comprimento médio $E(W)$ das palavras-código neste esquema é $E(W) = 1,5$, o que é vantajoso quando comparado com o comprimento médio das palavras-código resultantes da codificação homofônica clássica (Figura 2.5), que é $E(W) = 2$.

2.3.3 Parâmetros de Desempenho de um Codificador Homofônico

Define-se a expansão do texto claro em um sistema de codificação homofônica como $E(W) - H(U)$. No contexto da codificação de fonte [23], define-se a eficiência η do código

como

$$\eta = \frac{H(U)}{E(W)}. \quad (2.6)$$

Consequentemente, a redundância ρ é definida como

$$\rho = 1 - \eta = \frac{[E(W) - H(U)]}{E(W)}. \quad (2.7)$$

Define-se a taxa de transmissão de informação R de um sistema de codificação homofônica como o número de *bits* por símbolo produzido na saída de um canal homofônico. No contexto da codificação homofônica, seguem as seguintes definições para a eficiência η e a redundância ρ de um sistema de codificação homofônica.

Definição 2.3 *Define-se a eficiência η de um sistema de codificação homofônica como*

$$\eta = \frac{R}{E(W)}. \quad (2.8)$$

Definição 2.4 *Define-se a redundância ρ de um sistema de codificação homofônica como*

$$\rho = 1 - \eta = \frac{[E(W) - R]}{E(W)}. \quad (2.9)$$

Nos exemplos ilustrados pelas Figuras 2.5 e 2.6, o valor da taxa R coincide com o valor da entropia da fonte, ou seja, $R = H(U) = h\left(\frac{1}{4}\right) = 0,8113$, em que $h(\cdot)$ denota a função da entropia binária. Assim, a eficiência do esquema ilustrado pela Figura 2.5 é $\eta = 0,4056$, enquanto que a eficiência do esquema ilustrado pela Figura 2.6 é $\eta = 0,5409$, sendo 33,4% mais eficiente.

Definição 2.5 (Codificação Homofônica Perfeita) *Uma codificação homofônica é definida como perfeita se a palavra-código X_1, X_2, \dots, X_W for completamente aleatória, ou seja, se os símbolos D -ários X_i , $1 \leq i \leq W$, forem independentes e uniformemente distribuídos [4].*

Proposição 2.3 *Para o esquema de codificação homofônica ilustrado na Figura 2.4, tem-se*

$$H(U) \leq H(V) \leq E(W) \log D, \quad (2.10)$$

com igualdade à esquerda se e somente se o canal homofônico for determinístico, e com igualdade à direita se e somente se a técnica de codificação homofônica for perfeita. Existe uma codificação D -ária livre de prefixo de V de modo que o esquema é perfeito se e somente se $P(V = v_i) = D^{-l_i}$, para todos os valores v_i de V , em que l_i é o comprimento da palavra-código D -ária associada a v_i .

Demonstração: Para provar a desigualdade da direita $H(V) \leq E(W) \log D$, considere a entropia de V , dada por

$$H(V) = - \sum_{i=1}^L P_i \log P_i. \quad (2.11)$$

Sejam Q_1, Q_2, \dots, Q_L números reais tais que $Q_i \geq 0, \forall 1 \leq i \leq L$ e $\sum_{i=1}^L Q_i = 1$. Tomando-se a desigualdade fundamental da Teoria da Informação $\log r \leq (r - 1) \log e$ e fazendo $r = \frac{Q_i}{P_i}$, tem-se

$$\log \left(\frac{Q_i}{P_i} \right) \leq \left(\frac{Q_i}{P_i} - 1 \right) \log e.$$

Multiplicando os dois lados da inequação por P_i e somando sobre i tem-se

$$\begin{aligned} \sum_{i=1}^L P_i \log \left(\frac{Q_i}{P_i} \right) &\leq \sum_{i=1}^L P_i \left(\frac{Q_i}{P_i} - 1 \right) \log e = \left[\sum_{i=1}^L Q_i - \sum_{i=1}^L P_i \right] \log e = [1 - 1] \log e, \\ \sum_{i=1}^L P_i \log \left(\frac{Q_i}{P_i} \right) &\leq 0, \\ \sum_{i=1}^L P_i \log Q_i - \underbrace{\sum_{i=1}^L P_i \log P_i}_{H(V)} &\leq 0, \\ H(V) &\leq - \sum_{i=1}^L P_i \log Q_i. \end{aligned} \quad (2.12)$$

Como $\sum_{i=1}^L Q_i = 1$, pode-se escolher

$$Q_i = \frac{D^{-l_i}}{\sum_{j=1}^L D^{-l_j}}. \quad (2.13)$$

Substituindo a Equação 2.13 na Equação 2.12, obtém-se

$$\begin{aligned} H(V) &\leq - \sum_{i=1}^L P_i \log D^{-l_i} + \sum_{i=1}^L P_i \log \left(\sum_{j=1}^L D^{-l_j} \right), \\ H(V) - \log D \underbrace{\sum_{i=1}^L P_i l_i}_{E(W)} &\leq \log \left(\sum_{j=1}^L D^{-l_j} \right). \end{aligned}$$

Utilizando a desigualdade de Kraft $\sum_{i=1}^L D^{-l_i} \leq 1$, tem-se que

$$\log \left(\sum_{j=1}^L D^{-l_j} \right) \leq 0.$$

Assim,

$$H(V) - E(W) \log D \leq 0.$$

O que leva a

$$H(V) \leq E(W) \log D,$$

o que prova a desigualdade da direita. A igualdade em (2.12) ocorre quando $P_i = Q_i$, ou seja,

$$P_i = \frac{D^{-l_i}}{\sum_{j=1}^L D^{-l_j}}.$$

A codificação homofônica perfeita implica $\sum_{j=1}^L D^{-l_j} = 1$, o que leva a $P_i = D^{-l_i}$, $\forall 1 \leq i \leq L$.

Para provar a desigualdade da esquerda $H(U) \leq H(V)$, considere a regra da cadeia da incerteza, dada por

$$\begin{aligned} H(U, V) &= H(U) + H(V|U), \\ &= H(V) + H(U|V). \end{aligned}$$

Como a saída V do canal homofônico determina unicamente a entrada U , então $H(U|V) = 0$, o que leva a

$$H(V) = H(U) + H(V|U).$$

Como $H(V|U) \geq 0$, tem-se

$$H(V) \geq H(U),$$

o que prova a desigualdade da esquerda. Quando o canal é determinístico, ou seja, $H(V|U) = 0$, tem-se $H(V) = H(U)$. ■

Definição 2.6 (Codificação Homofônica Ótima) *Uma técnica de codificação homofônica é definida como ótima se ela for perfeita e sua redundância é a menor possível, ou seja, o comprimento médio $E(W)$ das palavras-código D -árias é o menor possível [4].*

Em 1990, H. N. Jendal, Y. J. B. Kuhn e J. L. Massey apresentaram uma técnica de codificação homofônica ótima, conhecida como técnica JKM [4]. Em [5], a técnica Rocha-Massey (RM) é apresentada, introduzindo uma cota superior relacionada ao número de lançamentos necessários para a escolha do homofonema na técnica JKM, quando $P_U(u_i)$ é decomposto como uma soma com um número infinito de termos. Em [6], é apresentada uma versão modificada da técnica JKM. Essa técnica apresenta uma construção sequencial de cada homofonema, concatenando palavras-código menores apropriadamente selecionadas, pertencentes a um conjunto finito, derivadas das probabilidades da fonte (que se supõe serem números racionais).

2.4 Codificação Homofônica Universal

Os esquemas de codificação homofônica mostrados nas seções anteriores requerem o conhecimento *a priori* da estatística da fonte de informação para realizar a codificação. A fim de lidar com casos em que tal conhecimento *a priori* não existe ou é de inviável obtenção, desenvolveram-se técnicas de codificação homofônica universal, que realizam a codificação sem a necessidade de estimar tal estatística. A Figura 2.7 ilustra a forma geral de codificação homofônica universal. Nesse esquema, a saída do gerador de símbolos aleatórios é utilizada para mapear aleatoriamente a saída da fonte de informação na sequência de texto claro de modo que ela possa ser recuperada sem o conhecimento do gerador. Dessa forma, quaisquer sequências particulares do texto claro se tornam possíveis substitutas (ou homofonemas) das sequências particulares da fonte de informação, sendo a escolha determinada pela sequência aleatória de saída do gerador. De modo geral, o mapeamento reversível deve ser responsável por tornar o texto claro completamente aleatório, caracterizando assim o esquema como um esquema de codificação homofônica perfeita.

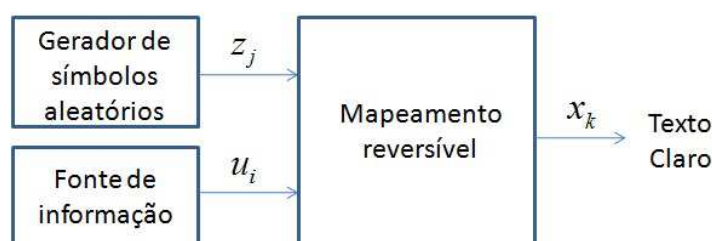


Figura 2.7: Forma geral de codificação homofônica universal.

2.4.1 O Codificador de Massey

Em [7], J. L. Massey sugeriu um esquema de codificação homofônica que utiliza como mapeamento reversível um multiplexador e um codificador universal de fonte, conforme ilustrado na Figura 2.8.

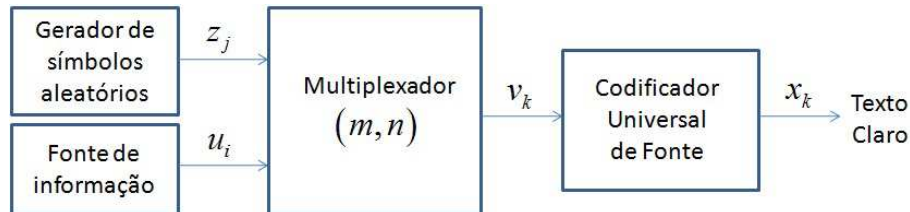


Figura 2.8: Codificador de Massey.

O multiplexador (m, n) considerado é um dispositivo que tem como saída blocos sucessivos de comprimento $m + n$, contendo m bits do gerador de símbolos aleatórios, seguidos de n bits da fonte de informação. Para $k = 0, 1, 2, \dots$, fazendo $k = q(m + n) + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < m + n$, a Equação 2.14 apresenta a expressão para a saída v_k do multiplexador:

$$v_k = \begin{cases} z_{qm+r}, & 0 \leq r < m, \\ u_{qn+r-m}, & m \leq r < m + n. \end{cases} \quad (2.14)$$

A saída do codificador é obtida processando a saída do multiplexador utilizando um esquema de codificação universal de fonte apropriado. A sequência original produzida pela fonte de informação pode ser recuperada a partir da saída do codificador homofônico, sem o conhecimento do gerador de símbolos aleatórios utilizado, simplesmente passando essa saída pelo decodificador universal de fonte correspondente e então descartando os símbolos aleatórios provenientes do gerador de símbolos aleatórios, de acordo com a Figura 2.9.

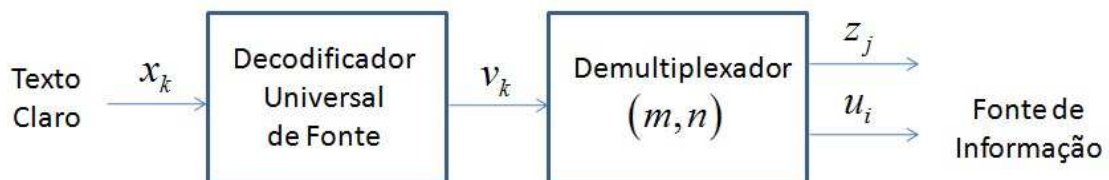


Figura 2.9: Decodificador de Massey.

Para $j = 0, 1, 2, \dots$, fazendo $j = qm + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < m$ e para $i = 0, 1, 2, \dots$, fazendo $i = sn + t$, em que $s = 0, 1, 2, \dots$ e $0 \leq t < n$, pode-se expressar as

saídas do demultiplexador como

$$z_j = v_{q(m+n)+r} \quad (2.15)$$

$$u_i = v_{s(m+n)+t+m} \quad (2.16)$$

Assumindo uma fonte de informação discreta, estacionária e ergódica (DSES), observa-se que a sequência de saída do multiplexador não representa em geral uma fonte DSES, uma vez que a multiplexação introduz não estacionaridade. No entanto, blocos de símbolos multiplexados, cujo comprimento seja um múltiplo de $m+n$, dão origem a um processo ciclo-estacionário. Essa condição é observada ao processar a sequência de saída do multiplexador com codificadores universais de fonte que possuam uma segmentação de símbolos de comprimento fixo, tais como o codificador Lynch-Davisson [24, 25] e o codificador Elias-Willems [26–28]. Por outro lado, essa condição não é observada ao processar essa sequência com codificadores universais de fonte que possuem segmentação de comprimento variável, como o codificador LZW [29–31].

A fonte de mensagens possui entropia dada por

$$H_\infty(V) = nH_\infty(U) + m, \quad (2.17)$$

em que $H_\infty(U)$ é a taxa de informação da fonte binária de informação.

Em [32], o esquema de Massey é analisado considerando o algoritmo LZW como codificador universal de fonte, seguindo duas estratégias:

1. Gerando o dicionário LZW ignorando a estrutura ciclo-estacionária dos blocos de comprimento $m+n$ na saída do multiplexador;
2. Desconsiderando o dicionário gerado no bloco anterior, de comprimento $m+n$, reiniciando a geração do dicionário a cada novo bloco.

Nos testes realizados, tendo como parâmetro de qualidade a entropia da sequência de saída do codificador homofônico, a estratégia 1 apresentou melhor desempenho quando comparada com a estratégia 2. Isso se deve ao fato de que, utilizando a estratégia 2, não há informação suficiente para que o codificador LZW aprenda a estatística em apenas um bloco de comprimento $m+n$.

Apesar de a sequência de saída do codificador de Massey apresentar uma alta entropia, ela possui diversos desvios estatísticos. Em [8], são apresentados os resultados de testes estatísticos realizados com a suíte de testes do NIST em sequências geradas pelo esquema de Massey, considerando fontes e parâmetros diferentes. Esses testes foram realizados quando o

codificador LZW e o codificador Lynch-Davisson são empregados. Nos dois casos as sequências geradas pelo codificador de Massey foram reprovadas na maioria dos testes estatísticos do NIST. Isso motivou o desenvolvimento de esquemas de codificação homofônica universal que gerassem sequências com propriedades estatísticas melhores.

2.4.2 O Codificador OMI

Como uma alternativa ao esquema sugerido por J. L. Massey em [7], foi proposto em [8] um outro esquema de codificação homofônica universal, o codificador *One-Time Pad - Multiplexer - Interleaver* (OMI) cuja forma geral está ilustrada na Figura 2.10.

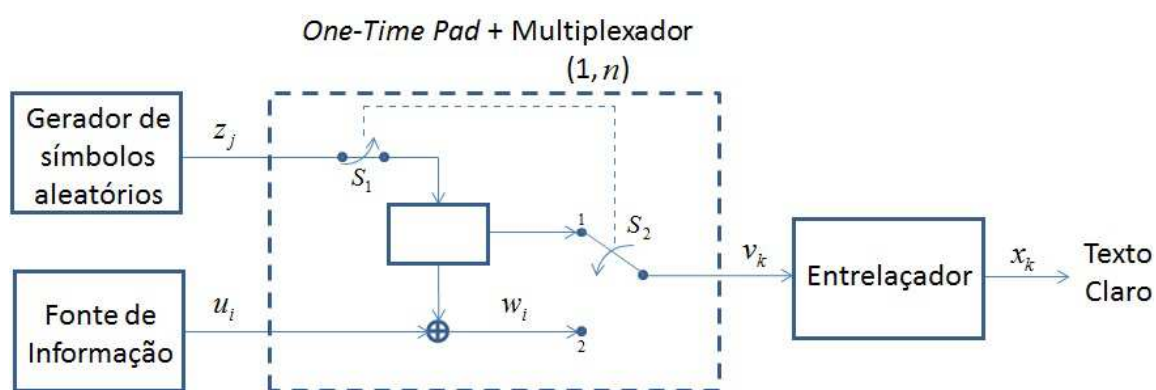


Figura 2.10: Codificador OMI.

Nesse esquema, w_i é o resultado da operação “ou exclusivo” entre um *bit* z_j proveniente do gerador de símbolos aleatórios (equiprováveis e estatisticamente independentes) e um *bit* u_i proveniente da fonte de informação. Para $i = 0, 1, 2, \dots$, fazendo $i = qn + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < n$, tem-se

$$w_i = u_i \oplus z_q. \quad (2.18)$$

O multiplexador tem como saída sucessivos blocos de comprimento $n + 1$ *bits*, contendo 1 *bit* do gerador de símbolos aleatórios seguido dos n *bits* do resultado da operação “ou exclusivo” entre o *bit* aleatório e um *bit* proveniente da fonte de informação. As chaves S_1 e S_2 operam de forma síncrona, mudando suas posições de forma sucessiva. Com S_1 fechada e S_2 na posição 1, o símbolo z_j é carregado no elemento de memória e na entrada do entrelaçador. Essa configuração de chaves opera durante um ciclo. Com S_1 aberta e S_2 na posição 2, o símbolo $w_i = u_i \oplus z_j$ é carregado na entrada do entrelaçador. Essa configuração de chaves opera durante n ciclos. Após os n ciclos, a chave S_1 fecha e a chave S_2 muda para a posição 1 e o processo reinicia. Para $k = 0, 1, 2, \dots$, fazendo $k = q(n + 1) + r$, em que $q = 0, 1, 2, \dots$

e $0 \leq r < n + 1$, tem-se a seguinte expressão para a saída do multiplexador:

$$v_k = \begin{cases} z_q, & r = 0, \\ w_{qn+r-1} = u_{qn+r-1} \oplus z_q, & r \neq 0. \end{cases} \quad (2.19)$$

Considerando $n = 1$, é bem conhecido que, para $i = 0, 1, 2, \dots$, a cifra binária *one-time pad* [22] tendo u_i como texto claro e z_i como chave secreta, tem $u_i \oplus z_i$ como a cifra de saída correspondente. A propriedade mais importante do *one-time pad* é a que se segue.

Propriedade 2.1 (Cifra de blocos descartáveis (*one-time pad*)) *Se Z for completamente aleatória, então a variável aleatória definida por $U \oplus Z$ também é completamente aleatória e não depende da distribuição de probabilidade de U .*

Além disso, nota-se que

$$P(Z = z_i, V = u_i \oplus z_i) = P(Z = z_i)P(V = u_i \oplus z_i | z_i) = P(Z = z_i)P(U = u_i). \quad (2.20)$$

Segue de (2.20) que, em geral, Z e $U \oplus Z$ não satisfazem à condição requerida para a independência estatística, ou seja, que $P(Z = z_i, V = u_i \oplus z_i) = P(Z = z_i)P(V = u_i \oplus z_i)$, exceto para o caso em que a fonte U já é completamente aleatória, o que naturalmente não necessita de codificação homofônica. Assim, o multiplexador emite pares $(z_i, u_i \oplus z_i)$ de símbolos binários em que tanto z_i quanto $u_i \oplus z_i$ são completamente aleatórios, porém não necessariamente estatisticamente independentes. Para lidar com esta possível dependência estatística entre os pares $(z_i, u_i \oplus z_i)$ faz-se o uso de um entrelaçador. Assim, a saída do codificador é obtida processando a saída do multiplexador utilizando um entrelaçador apropriado, sendo expressa por $x_k = v_{\pi(k)}$, em que $\pi(\cdot)$ denota a função de permutação do entrelaçador. A sequência original pode ser recuperada processando a saída do codificador homofônico de acordo com a Figura 2.11.

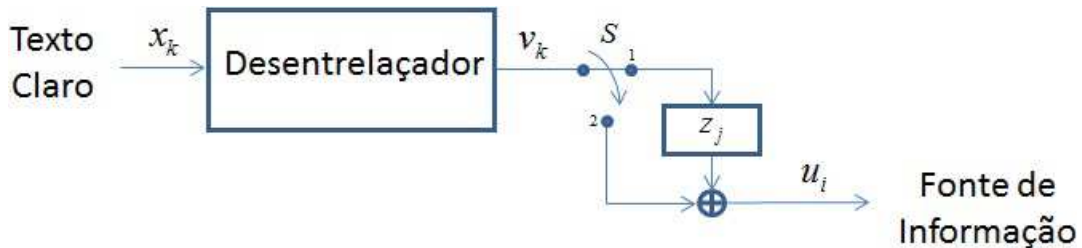


Figura 2.11: Decodificador OMI.

A chave S inicia a operação na posição 1 para carregar o *bit* proveniente do gerador de símbolos aleatórios no elemento de memória (primeiro *bit* do bloco de $n + 1$ *bits*). Ela fica na

posição 1 durante um ciclo e em seguida muda para a posição 2, permanecendo nela por n ciclos. Com a chave nessa posição, a operação “ou exclusivo” é realizada entre o *bit* aleatório armazenado no elemento de memória e um *bit* proveniente do desentrelaçador, resultando assim um *bit* da fonte de informação. Após os n ciclos, a chave S muda para a posição 1 e o processo reinicia.

A saída do desentrelaçador é expressa por $v_k = x_{\pi^{-1}(k)}$, em que $\pi^{-1}(\cdot)$ denota a função inversa de permutação do entrelaçador. Para $i = 0, 1, 2, \dots$, fazendo $i + 1 = q(n + 1) + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < n + 1$, pode-se expressar a saída do decodificador homofônico como

$$u_i = v_{q(n+1)} \oplus v_{q(n+1)+r+1}. \quad (2.21)$$

A taxa R do codificador OMI é dada por

$$R = \frac{n}{n+1} = \frac{1}{1 + \frac{1}{n}}. \quad (2.22)$$

Quando $n \rightarrow \infty$, tem-se $R \rightarrow 1$. Considerando uma fonte de informação U previamente comprimida por um codificador de fonte ideal, a taxa é dada por

$$R = \frac{1}{1 + \frac{1}{nH(U)}}. \quad (2.23)$$

Em [9], o codificador OMI é analisado, considerando $n = 1$ e utilizando a versão quadrada do entrelaçador de Berrou-Glavieux ($M = N \in \{32, 64\}$). Utilizou-se a suíte de testes estatísticos do NIST para testar a aleatoriedade da sequência de saída do codificador considerando diferentes fontes de informação. Os resultados obtidos com esse codificador foram consideravelmente melhores dos que os obtidos com o codificador de Massey utilizando o código LZW e o código de Lynch-Davisson como codificadores de fonte.

Em [8], esse esquema é analisado também considerando a versão quadrada do entrelaçador de Berrou-Glavieux ($M = N \in \{8, 16, 32, 64, 128, 256\}$), variando n no intervalo $1 \leq n \leq 15$. Os resultados obtidos com a suíte de testes estatísticos do NIST indicam que é possível realizar uma codificação homofônica eficiente atingindo taxas de até $\frac{15}{16} = 0,9375$, que é um valor bem próximo de 1, o que torna esse esquema bem interessante.

Em [33], esse codificador é analisado, considerando $n = 1$ e utilizando diversos entrelaçadores: a versão quadrada do entrelaçador de Berrou-Glavieux, do JPL e do LRTB e também os entrelaçadores Co-Primo, Takeshita-Costello e Welch-Costas. Foram considerados os períodos (em *bits*) $T \in \{64, 256, 1.024, 4.096, 16.384, 65.536e262.144\}$. Constatou-se a influência do

período dos entrelaçadores no desempenho da codificação. Constatou-se também fraquezas estatísticas presentes em alguns entrelaçadores, identificadas pelas reprovações persistentes em testes específicos do NIST, desqualificando-os para a aplicação.

2.4.3 O Codificador DEI

Um outro esquema universal de codificação homofônica é o codificador *Differential Encoder - Interleaver* (DEI), proposto em [10] e ilustrado na Figura 2.12.

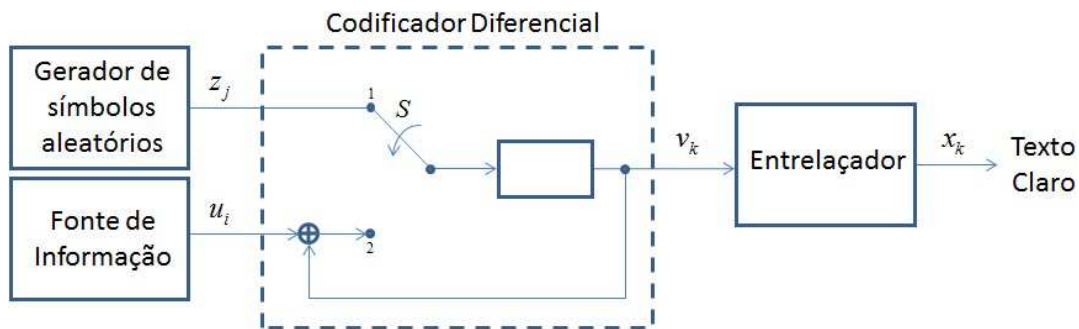


Figura 2.12: Codificador DEI.

O codificador diferencial tem como saída sucessivos blocos de comprimento $n + 1$ bits, em que o primeiro bit é proveniente do gerador de símbolos aleatórios. A chave S muda sua posição de forma sucessiva. Com S na posição 1, o símbolo z_j é carregado no elemento de memória e na entrada do entrelaçador. A chave opera nessa posição durante um ciclo. Com S na posição 2, é carregado no elemento de memória e também no entrelaçador o resultado da operação “ou exclusivo” entre um bit da fonte de informação e o bit previamente armazenado na memória. A chave opera nessa posição durante n ciclos. Após os n ciclos, a chave S muda para a posição 1 e o processo reinicia. Para $k = 0, 1, 2, \dots$, fazendo $k = q(n + 1) + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < n + 1$, tem-se a seguinte expressão para a saída do codificador diferencial:

$$v_k = \begin{cases} z_q, & r = 0, \\ u_{k-q-1} \oplus v_{k-1}, & r \neq 0. \end{cases} \quad (2.24)$$

Quando $n = 1$, o codificador diferencial também se transforma na cifra binária *one-time pad* [22]. Conforme discutido na Subseção 2.4.2, o codificador diferencial emite pares $(z_i, u_i \oplus z_i)$ de símbolos binários em que tanto z_i quanto $u_i \oplus z_i$ são completamente aleatórios, porém não necessariamente estatisticamente independentes. Assim, nesse caso também se emprega um entrelaçador para lidar com esta possível dependência estatística entre os pares

$(z_i, u_i \oplus z_i)$. Logo, a saída do codificador DEI é obtida processando a saída do codificador diferencial utilizando um entrelaçador apropriado, sendo expressa por $x_k = v_{\pi(k)}$, em que $\pi(\cdot)$ denota a função de permutação do entrelaçador. A sequência original pode ser recuperada processando a saída do codificador homofônico de acordo com a Figura 2.13.

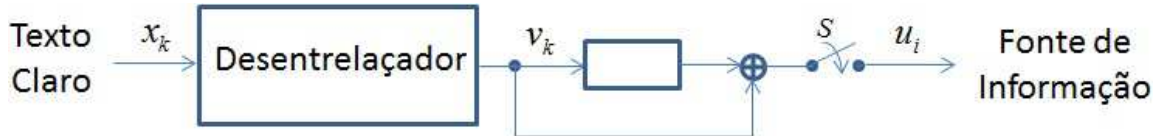


Figura 2.13: Decodificador DEI.

A chave S inicia a operação aberta para carregar o *bit* proveniente do desentrelaçador no elemento de memória. Ela fica aberta durante um ciclo e em seguida fecha, permanecendo nessa condição por n ciclos. Com a chave nessa posição, a operação “ou exclusivo” é realizada entre o *bit* armazenado no elemento de memória e um *bit* proveniente do desentrelaçador, resultando assim um *bit* da fonte de informação. Após os n ciclos, a chave S abre e o processo reinicia.

A saída do desentrelaçador é expressa por $v_k = x_{\pi^{-1}(k)}$, em que $\pi^{-1}(\cdot)$ denota a função inversa de permutação do entrelaçador. Para $i = 0, 1, 2, \dots$, fazendo $i = qn + r$, em que $q = 0, 1, 2, \dots$ e $0 \leq r < n$, pode-se expressar a saída do decodificador homofônico como

$$u_i = v_{q(n+1)+r} \oplus v_{q(n+1)+r+1}. \quad (2.25)$$

A taxa do codificador DEI é a mesma taxa do codificador OMI (Equação 2.22), de modo que, em relação a esse parâmetro, eles possuem desempenho idêntico.

Em [10] e em [11], o codificador DEI é analisado, considerando $1 \leq n \leq 15$ e utilizando o entrelaçador de Berrou-Glavieux com $M = N \in \{8, 16, 32, 64, 128, 256\}$. Utilizou-se a suíte de testes estatísticos do NIST para testar a aleatoriedade da sequência de saída do codificador considerando diferentes fontes de informação. Mostrou-se que, considerando esse entrelaçador, os resultados obtidos foram tão bons quanto os obtidos com o codificador OMI [9].

Neste trabalho é realizado uma análise envolvendo versões retangulares (mais gerais) dos entrelaçadores de Berrou-Glavieux, JPL e LRTB e também envolvendo uma variação maior dos parâmetros dos entrelaçadores Co-Primo, Takeshita-Costello e Welch-Costas. Para os codificadores OMI e DEI, a análise considera o parâmetro n no intervalo $1 \leq n \leq 15$ e aprimora os critérios de interpretação dos ensaios estatísticos do NIST.

CAPÍTULO 3

GERAÇÃO DE NÚMEROS PSEUDO-ALEATÓRIOS

3.1 Introdução

A segurança de diversos sistemas criptográficos depende fortemente da geração de números, *bits* ou símbolos de forma não previsível. Esses sistemas são bastante sensíveis às propriedades de tais geradores. Como exemplos podem ser citados a geração de chaves no algoritmo de cifragem DES, a geração dos números primos p e q no cripto-sistema RSA, esquemas de assinatura digital e alguns protocolos criptográficos que requerem a geração de números aleatórios em vários pontos [34].

O gerador de números aleatórios também encontra aplicação na codificação homofônica. Na sua versão clássica, um símbolo da mensagem original é substituído por um homofonema pertencente a um alfabeto maior. A escolha do homofonema a ser utilizado para representar o símbolo é feita de maneira aleatória. Na sua versão universal, faz-se uso de um gerador de números aleatórios para formar as palavras de texto claro, combinando os símbolos gerados pela fonte aleatória com os símbolos da fonte de informação através de um mapeamento reversível.

Uma sequência de *bits* estatisticamente independentes e uniformemente distribuídos pode ser interpretada como o resultado de lançamentos de uma moeda perfeita cujas faces podem ser associadas aos números 0 e 1, e cujas probabilidades de ocorrência são $P(0) = P(1) = \frac{1}{2}$. Além disso, cada lançamento da moeda é independente de todos os outros, ou seja, o resultado de qualquer lançamento anterior da moeda não afeta resultados obtidos em lançamentos

futuros. Assim, não é possível realizar a previsão do próximo elemento da sequência com probabilidade maior que $\frac{1}{2}$, não importando quantos elementos já foram produzidos; propriedade conhecida como imprevisibilidade [12]. Entretanto, é impossível produzir uma sequência infinita verdadeiramente aleatória em uma máquina com um número finito de estados, pois tal sequência seria necessariamente periódica, tornando-se assim previsível.

Existem dois tipos de geradores utilizados para produzir sequências aleatórias: os geradores de números aleatórios (RNGs) e os geradores de números pseudo-aleatórios (PRNGs).

3.2 Geradores de Números Aleatórios (RNGs)

Os geradores de números estatisticamente independentes e uniformemente distribuídos utilizam uma fonte não-determinística e uma função adequada para produzir a sequência, utilizando uma técnica conhecida como *de-skewing* [34]. A fonte não-determinística consiste de alguma grandeza física (gerada por *hardware*) ou ainda de processos utilizados pelo usuário (gerada por *software*). Essa fonte está sujeita à influência de fatores externos e também ao mau funcionamento, de modo que os números de saída podem estar *polarizados* (não equiprováveis), ou *correlacionados* (a probabilidade de a fonte emitir um determinado número depende dos números emitidos anteriormente). O uso da técnica *de-skewing* é requerido para retirar qualquer fraqueza da fonte que resulta na produção de números não-aleatórios, por exemplo, a ocorrência de uma sequência longa de 0's ou de 1's. Um gerador bem projetado deve utilizar tantas boas fontes não-determinísticas quanto for possível. O uso de diversas fontes previne contra a possibilidade de algumas delas falharem, serem observadas ou manipuladas por um adversário. Cada fonte deve ser amostrada e as sequências resultantes devem ser combinadas utilizando funções de mistura complexas, para extrair os números verdadeiramente aleatórios a partir dessas sequências.

Os RNGs baseados em *hardware* exploram a aleatoriedade que ocorre em fenômenos físicos, tais como:

- O ruído térmico em um circuito elétrico, diodo ou resistor;
- Os efeitos quânticos em um semicondutor;
- O tempo decorrido entre a emissão de partículas durante um decaimento radioativo;
- A instabilidade da frequência de um oscilador.

Os RNGs baseados em *software* podem utilizar os seguintes processos:

- Relógio do sistema;
- Tempo entre teclas apertadas ou entre movimentos do *mouse*;
- Conteúdo da entrada ou saída dos *buffers* do sistema;
- Valores do sistema operacional tais como carga do sistema e estatísticas de rede.

O comportamento desses processos pode variar de acordo com a plataforma computacional utilizada.

Os RNGs devem ter essas três propriedades [35]:

1. Sua saída deve parecer aleatória. Tais geradores devem passar em todos os testes estatísticos de aleatoriedade existentes;
2. Sua saída deve ser imprevisível. Dado o completo conhecimento do algoritmo ou do *hardware* que gera a sequência e ainda dada toda a sequência gerada anteriormente, a previsão do próximo número a ser gerado deve ser computacionalmente inviável;
3. O gerador não pode ser reproduzido confiavelmente. Aplicando exatamente a mesma entrada duas vezes no gerador resulta em duas sequências aleatórias não relacionadas, completamente diferentes.

A propriedade 3 implica uma dificuldade de determinar se a sequência gerada é realmente aleatória. Por isso, tais geradores devem ser testados de vez em quando, utilizando testes de aleatoriedade adequados.

Idealmente, algoritmos e protocolos criptográficos seguros devem ser gerados utilizando RNGs, que não devem estar sujeitos à observação ou manipulação por um usuário não autorizado do sistema. Entretanto, a geração de números aleatórios é um procedimento ineficiente na maioria dos casos práticos. O armazenamento e a transmissão segura de números aleatórios quando eles são requeridos em aplicações tais como por exemplo o *one-time pad* se tornam inviáveis para grandes quantidades. Em tais situações, é preferível utilizar um gerador de números pseudo-aleatórios em vez de um RNG.

3.3 Geradores de Números Pseudo-Aleatórios (PRNGs)

Este tipo de gerador utiliza uma ou mais entradas, também chamadas de sementes, para gerar uma sequência periódica de números. Cada elemento da sequência é reproduzido a partir da semente. Assim, apenas a semente precisa ser guardada para realizar a reprodução de uma sequência pseudo-aleatória. Os PRNGs possuem as propriedades 1 e 2, citadas na Subseção 3.2. Se uma mesma semente for aplicada duas vezes no PRNG, as suas saídas consistirão em duas sequências completamente idênticas. Essa característica é interessante na criptografia e permite a realização de ensaios em que a sequência de saída do PRNG precise ser bem determinada.

Se a semente for desconhecida, o próximo número da sequência deve ser imprevisível apesar do conhecimento de quaisquer números anteriores da sequência (*imprevisibilidade anterior*) [12]. Um PRNG pode obter sementes a partir da saída de um RNG. A saída de um PRNG é uma função determinística da semente (por isso o nome pseudo-aleatório), ou seja, toda a aleatoriedade depende da geração das sementes. Além disso, a partir do conhecimento de quaisquer números gerados pelo PRNG, é inviável determinar a semente utilizada (*imprevisibilidade posterior*) [12]. Nenhuma correlação entre a semente e qualquer valor gerado a partir dela deve ser evidente. Deve-se tomar cuidado na obtenção das sementes, sabendo-se que a sequência produzida pelo PRNG é completamente previsível uma vez que a semente e o algoritmo de geração sejam conhecidos. Como os algoritmos de geração são disponíveis publicamente, a semente deve ser secreta, seguindo o mesmo princípio aplicado aos criptosistemas. O período do PRNG deve ser grande o bastante para que, na aplicação considerada, a sequência gerada não se repita, parecendo assim aleatória. Por exemplo, se é preciso um milhão de *bits* em uma aplicação, são impróprias as escolhas de PRNGs com período de 100 mil *bits*.

Em uma sequência pseudo-aleatória com propriedades estatísticas satisfatórias, cada valor da sequência é produzido a partir de valores produzidos previamente utilizando transformações que introduzem uma aparente aleatoriedade à sequência. Essas transformações eliminam as correlações estatísticas entre a entrada e a saída, resultando em uma sequência de saída com propriedades estatísticas mais satisfatórias. Para se ganhar confiança de que os PRNGs são seguros, eles devem ser sujeitos a uma variedade de testes estatísticos que detectam características que se esperam estar presentes nas sequências aleatórias. Neste trabalho, para testar a aleatoriedade do gerador implementado, é utilizada uma suíte de 15 testes de aleatoriedade

proposta pelo NIST [12] (vide Capítulo 5).

Boa parte dos PRNGs utilizam aritmética modular para gerar suas sequências de saída [36]. Como exemplos, podem ser citados:

1. Gerador congruencial linear: Produz uma sequência pseudo-aleatória x_1, x_2, x_3, \dots de acordo com a equação

$$x_n = (ax_{n-1} + b) \pmod{p}, \quad n \geq 1, \quad (3.1)$$

em que x_0 é a semente e a, b e p são parâmetros que caracterizam o gerador.

2. Gerador congruencial linear multivariável: Generalização do gerador congruencial linear. A sequência de saída é descrita pela equação

$$x_n = (a_1x_{n-1} + a_2x_{n-2} + \dots + a_kx_{n-k} + b) \pmod{p}, \quad n \geq k. \quad (3.2)$$

3. Gerador congruencial quadrático: A sequência de saída é descrita pela equação

$$x_n = (ax_{n-1}^2 + bx_{n-1} + c) \pmod{p}, \quad n \geq 1. \quad (3.3)$$

Entretanto, Plumstead [37] mostrou que, dados apenas alguns poucos elementos da sequência de saída de um gerador congruencial linear, pode-se prever o restante da sequência, mesmo quando os parâmetros a, b e p são desconhecidos. Boyar [38] estendeu o método de Plumstead e mostrou que os geradores congruenciais lineares multivariável e os geradores congruenciais quadráticos são criptograficamente inseguros. Finalmente, Krawczyk [39] generalizou esses resultados e mostrou como a saída de qualquer gerador congruencial polinomial multivariável pode ser prevista eficientemente.

Assim, pelo fato de serem previsíveis, os geradores congruenciais apresentados são completamente inseguros para propósitos criptográficos. Porém, tais geradores são comumente usados em simulações, uma vez que suas sequências de saída passam facilmente em testes estatísticos. Por este motivo, para realizar as simulações dos sistemas abordados neste trabalho, foi escolhido como PRNG o gerador congruencial de Park-Miller-Carta (PMC) (versão otimizada sugerida por D. Carta do gerador de Park-Miller). Além do fato de que a sequência de saída do gerador passa em todos os testes de aleatoriedade do NIST (vide Seção 6.1), outros motivos para a escolha desse gerador são a simplicidade de sua implementação e a rápida geração da sequência de saída (vide Seção 3.5).

3.4 O gerador Congruencial Linear de Park-Miller

3.4.1 Descrição do Gerador

Em 1951, D. H. Lehmer propôs um procedimento de geração de números aleatórios bastante satisfatório, chamado de gerador congruencial linear multiplicativo [40]. O algoritmo envolve a escolha de dois parâmetros inteiros fixos:

1. Módulo p : Um número primo grande.
2. Multiplicador a : Um número inteiro compreendido entre 2 e $p - 1$.

A geração da sequência de números inteiros x_1, x_2, x_3, \dots é feita pela equação iterativa

$$x_{n+1} = f(x_n), \quad \text{para } n = 0, 1, 2, \dots \quad (3.4)$$

A função geradora $f(\cdot)$ é definida para todo x compreendido entre 1 e $p - 1$. Sua forma geral é

$$f(x) = ax \pmod{p}. \quad (3.5)$$

A sequência de números deve ser iniciada escolhendo uma *semente inicial* x_0 , compreendida entre 1 e $p - 1$. A escolha de um número primo para o módulo p se deve ao fato de que todos os números compreendidos entre 1 e $p - 1$ são relativamente primos com p , ou seja, $\text{mdc}(x_i, p) = 1, \forall 1 \leq x_i \leq p - 1$, sendo x_i um número inteiro. Isso evita que a sequência se torne nula em algum ponto.

A sequência x_1, x_2, x_3, \dots pode dar origem a uma sequência u_1, u_2, u_3, \dots , normalizada no intervalo $[0, 1]$, realizando a divisão

$$u_n = \frac{x_n}{p} \quad \text{para } n = 1, 2, \dots \quad (3.6)$$

A aleatoriedade gerada pela sequência x_1, x_2, x_3, \dots não é afetada quando se faz a normalização, sendo herdada pela sequência resultante. É importante notar que os valores $u = 0$ e $u = 1$ não ocorrem nunca; o menor valor possível para u é $\frac{1}{p}$, enquanto que o maior valor é $1 - \frac{1}{p}$.

Um outro aspecto interessante a ser analisado é o período da sequência gerada em função do multiplicador a . O período da sequência gerada considerando um determinado multiplicador é um divisor de $p - 1$. Em aplicações criptográficas, é interessante utilizar sequências com o maior período possível, denominadas sequências de período máximo. Nesse caso, o período é exatamente $p - 1$. Para um dado módulo p , existe uma porcentagem significativa das $p - 2$

escolhas possíveis de a que geram uma sequência de período máximo. Para uma dada função geradora de período máximo, qualquer semente inicial entre 1 e $p - 1$ pode ser escolhida sem afetar a aleatoriedade da sequência gerada. O resultado gerado é apenas um deslocamento cíclico do resultado gerado pela semente $x_0 = 1$.

Os números da forma $M_n = 2^n - 1$, $n \geq 1$, são chamados de *Números de Mersenne* [41], em homenagem ao matemático francês Marin Mersenne (1588-1648). Aqueles números de Mersenne que por ventura vierem a ser primos são conhecidos como *Primos de Mersenne*. Em [40], Lehmer sugeriu o primo de Mersenne $p = 2^{31} - 1 = 2147483647$ como uma escolha apropriada para o módulo. Na implementação realizada desse gerador, esse módulo é bastante adequado, uma vez que o compilador utilizado para implementar o gerador trabalha com uma aritmética de 32 *bits*.

Tendo fixado o módulo $p = 2^{31} - 1$, o próximo passo é encontrar bons multiplicadores a de forma a atender positivamente as três seguintes questões:

Q_1 : $f(x) = ax \pmod{p}$ é uma função geradora de período máximo?

Q_2 : A sequência de período máximo $\dots, x_1, x_2, \dots, x_{p-1}, x_1, \dots$ passa nos testes de aleatoriedade?

Q_3 : A função $f(\cdot)$ pode ser implementada eficientemente utilizando uma aritmética de 32 *bits*?

Cada uma dessas três questões serve como um filtro que limita as escolhas possíveis de a . Sabe-se que, para $p = 2^{31} - 1$, dos mais de 2 bilhões de escolhas possíveis para a , apenas uma pequena parcela delas passa em todos os três testes, ou seja, responde as três questões afirmativamente. Em 1969, Lewis, Goodman e Miller sugeriram o multiplicador $a = 7^5 = 16807$ baseados no fato de que

$$f(x) = 16807x \pmod{2147483647} \quad (3.7)$$

é uma função geradora de período máximo [42]. A teoria envolvida nas três questões pode ser vista no Apêndice A.

Diversos testes de aleatoriedade de período máximo para esse gerador foram desenvolvidos e são amplamente discutidos em [36] e [43]. Para reforçar ainda mais, utilizando a Equação (3.7) normalizada para o intervalo $[0, 1]$ (Equação (3.6)), gerou-se 5 sequências binárias, utilizando 5 sementes diferentes: $x_{01} = 12345$, $x_{02} = 54321$, $x_{03} = 112358$, $x_{04} = 19872008$ e $x_{05} = 26011982$. Cada uma dessas sequências consiste em 500 subsequências de 2^{20} *bits*, e

foram submetidas aos testes de aleatoriedade adotados pelo NIST, cuja descrição resumida se encontra na Seção 5.1. O resultado de tais testes, realizados é mostrado na Seção 5.2.

Em 1979, L. Schrage demonstrou que esse gerador pode ser implementado corretamente sem a ocorrência de *overflow* [44], podendo a máquina representar todos os números inteiros no intervalo de -2^{31} até $2^{31} - 1$. Assim, os parâmetros $a = 16807$ e $p = 2^{31} - 1$ definem um gerador de período máximo adequado às aplicações consideradas neste trabalho.

3.5 Otimizações na Implementação do Gerador

Esta seção trata de uma implementação rápida utilizando uma aritmética de 32 *bits*, idealizada por Carta [20], do gerador linear congruencial de números aleatórios discutido na Seção 3.4. A idéia principal é realizar a implementação do gerador definido pela Equação 3.7, sem efetuar operações de divisão, que são bastante lentas quando comparadas com a operação de adição.

Na representação de números inteiros em 32 *bits*, os registradores utilizam 1 *bit* para o sinal e 31 *bits* para a magnitude do número. O processo de geração de um número aleatório discutido na Seção 3.4 efetua uma multiplicação para, em seguida, efetuar uma divisão e tomar o seu resto. A partir deste momento, é utilizado o prefixo "0x" antes do número para indicar o uso da notação hexadecimal.

Considere o caso de maior magnitude na multiplicação, em que $a = 16807 = 0x41A7$ e $x_i = 2^{31} - 2 = 0xFFFFFE$. Multiplicando esses dois termos, tem-se $ax_i = 36092757638322 = 0x20D37FFF7CB2$. Note que precisa-se de 46 *bits*, ou seja, de 2 registradores de 32 *bits* para representar o resultado da multiplicação, como ilustra a Figura 3.1.

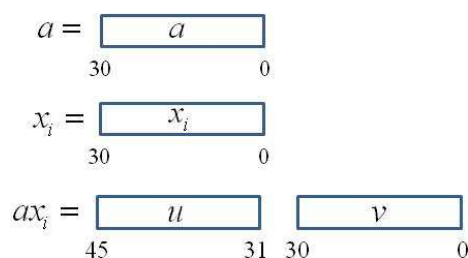


Figura 3.1: Representação do produto de dois números inteiros como registradores adjacentes de 32 bits.

Assim como a Figura 3.1 ilustra, considere v , possuindo 31 *bits* (do *bit* 0 da multiplicação até o *bit* 30) e u , possuindo 15 *bits* (do *bit* 31 da multiplicação até o *bit* 45). Tomando como

base a Equação (3.7), pode-se escrever:

$$\begin{aligned}
 x_{n+1} &= ax_n \pmod{2^{31} - 1}, \\
 &= v + u \cdot 2^{31}, \\
 &= v + u \cdot (2^{31} - 1) + u.
 \end{aligned} \tag{3.8}$$

Como é necessário realizar a operação módulo por $2^{31} - 1$, pode-se simplesmente eliminar o termo $u \cdot (2^{31} - 1)$ da Equação (3.8), resultando em

$$x_{n+1} = u + v. \tag{3.9}$$

Assim, a Equação (3.9) indica que, em vez de realizar a operação de divisão, precisa-se apenas somar os 15 *bits* menos significativos dos registradores u e v , mantendo os demais *bits* de v intactos.

Como exemplo, considere $p = 2^{31} - 1$, $a = 16807$ e $x_i = 123456789$. $ax_i = 2074938252723 = 0x1E31BF51DB3$. Assim, tem-se:

v	0011011111101010001110110110011
u	0001111000110
$u + v$	001101111110101001000101111001

Deste modo, $ax_1 \pmod{2^{31} - 1} = u + v = 469049721 = 0x1BF52179$. Enfim, esta foi a otimização utilizada na implementação do gerador de números pseudo-aleatórios.

CAPÍTULO 4

FUNDAMENTOS DE ENTRELAÇADORES

4.1 Introdução

O entrelaçador é um dispositivo de uma única entrada e uma única saída, para o qual a sequência de símbolos, de um determinado alfabeto \mathbf{A} , na entrada, produz uma sequência de saída com os mesmos símbolos de \mathbf{A} em uma ordem temporal diferente. Esse dispositivo é bastante utilizado na área de códigos controladores de erros, tendo como principal objetivo tornar aleatórias as posições dos erros inseridos durante a transmissão [21], combatendo erros em surto e permitindo a utilização de códigos corretores de erros aleatórios, como códigos convolucionais, por exemplo.

Um entrelaçador pode ser descrito, de uma maneira geral, como está ilustrado na Figura 4.1.

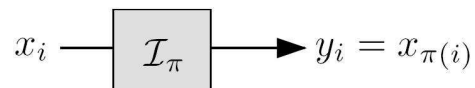


Figura 4.1: Modelo de um entrelaçador.

A operação realizada no tempo i é descrita utilizando a seguinte notação: a saída do entrelaçador no instante i , denotada por $y_i \in \mathbf{A}$, é a $\pi(i)$ -ésima entrada $x_{\pi(i)}$. Tomando sequências, diz-se que $y = \mathcal{J}_\pi(x)$. Assim, o entrelaçador \mathcal{J}_π é descrito pela função inversível $\pi : \mathbb{Z} \rightarrow \mathbb{Z}$, que é uma permutação no conjunto \mathbb{Z} dos números inteiros. O desentrelaçador para um dado entrelaçador \mathcal{J}_π é um entrelaçador \mathcal{J}_μ tal que $\mathcal{J}_\mu = \mathcal{J}_\pi^{-1}$.

A fim de ser realizável na prática, um entrelaçador necessita ser periódico, com um período finito T .

Definição 4.1 *Um entrelaçador é dito periódico de período T se sua função de permutação satisfaz*

$$\pi(i) - T = \pi(i - T), \quad (4.1)$$

para todo i .

Sendo periódico com período T , um entrelaçador pode ser representado por uma matriz, que informa a posição $\pi(i)$ de T números inteiros, como ilustrado em (4.2). Essa matriz é denominada permutação fundamental do entrelaçador, e pode ser expandida, de modo a abranger todos os valores de $i \in \mathbb{Z}$ [21].

$$\begin{pmatrix} 0 & 1 & \cdots & T-1 \\ \pi(0) & \pi(1) & \cdots & \pi(T-1) \end{pmatrix} \quad (4.2)$$

O entrelaçador cuja permutação fundamental é definida como (4.2), é chamado de entrelaçador de bloco. Outra forma de representar um entrelaçador de bloco é por meio da função de permutação $\pi(i)$, $0 \leq i < T$, que determina a posição de cada um dos i -ésimos símbolos de entrada. Essa é a representação adotada neste trabalho.

4.2 A Dispersão de um Entrelaçador

A dispersão é uma medida de “aleatoriedade” de um entrelaçador. Ela é um parâmetro normalizado que pode assumir valores entre 0 (ou aproximadamente 0) e 1.

Definição 4.2 (Conjunto dos vetores de deslocamento) *Define-se o conjunto $\mathcal{D}(\mathcal{J})$ dos vetores de deslocamento como*

$$\mathcal{D}(\mathcal{J}) = \{(\Delta_x, \Delta_y) \in \mathbb{Z}^2 \mid \Delta_x = j - i, \Delta_y = \pi(j) - \pi(i), 0 \leq i < j < T\}. \quad (4.3)$$

Definição 4.3 (Dispersão de um Entrelaçador) *Define-se a dispersão do entrelaçador, denotada por Γ , como a cardinalidade do conjunto $\mathcal{D}(\mathcal{J})$, ou seja, $\Gamma = |\mathcal{D}(\mathcal{J})|$.*

A dispersão satisfaz a desigualdade $T - 1 \leq \Gamma \leq \frac{T(T-1)}{2}$.

Definição 4.4 (Dispersão normalizada) *Define-se a dispersão normalizada do entrelaçador, denotada por γ , como*

$$\gamma = \frac{2\Gamma}{T(T-1)}. \quad (4.4)$$

A dispersão normalizada do entrelaçador assume valores entre $\frac{2}{T}$ e 1 (quando T é grande, o limite inferior é aproximadamente zero) [21].

Definição 4.5 (Conjunto dos vetores de deslocamento - Definição alternativa) *Define-se alternativamente o conjunto dos vetores de deslocamento como*

$$\mathcal{D}(\mathcal{J}) = \{(\Delta_x, \Delta_y) \in \mathbb{Z}^2 \mid 1 \leq \Delta_x \leq T-1, \Delta_y = \pi(j) - \pi(i), j = i + \Delta_x, 0 \leq i \leq T-1 - \Delta_x\}. \quad (4.5)$$

Nesse caso, $\mathcal{D}(\mathcal{J})$ pode ser representado como a união de $T-1$ conjuntos disjuntos, cada um deles associado a um dos $T-1$ valores possíveis de Δ_x . Assim, $\mathcal{D}(\mathcal{J}) = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{T-1}\}$, em que $\mathcal{C}_k = \{(k, \Delta_y) \in \mathbb{Z}^2 \mid \Delta_y = \pi(j) - \pi(i), j = i + k, 0 \leq i \leq T-1 - k\}$ e $1 \leq k \leq T-1$. Como os conjuntos \mathcal{C}_i e \mathcal{C}_j são disjuntos, $\forall 1 \leq i < j \leq T-1$, então é possível calcular $|\mathcal{D}(\mathcal{J})|$ de forma paralela, pois

$$|\mathcal{D}(\mathcal{J})| = \sum_{i=1}^{T-1} |\mathcal{C}_i|. \quad (4.6)$$

4.3 O Espalhamento de um Entrelaçador

Definição 4.6 (Fatores de espalhamento) *Diz-se que um entrelaçador possui fatores de espalhamento (s, t) se toda vez que $|i - j| < s$, então $|\pi(i) - \pi(j)| \geq t$. Outra forma de expressar essa definição é que toda vez que $|\pi(i) - \pi(j)| < t$, então $|i - j| \geq s$.*

Os símbolos individuais em um surto de comprimento t na entrada do entrelaçador são separados em blocos distintos de comprimento maior ou igual a s [21].

Um dado entrelaçador pode possuir mais de um par de fatores de espalhamento. Considere, por exemplo, um entrelaçador que é definido como uma matriz $N \times M$, em que os símbolos são escritos nas linhas e lidos através das colunas, da esquerda para a direita e de cima para baixo. A Figura 4.2 apresenta os gráficos de espalhamento desse entrelaçador quando $N = M = 4$. Nesses gráficos, um ponto é ilustrado para cada par $(i, \pi(i))$: o eixo das abscissas representa a variável i , enquanto que o eixo das ordenadas representa a variável $\pi(i)$. Em torno de cada ponto está ilustrado um quadrilátero de largura $(2s - 1)$ e altura $(2t - 1)$, centrado no próprio ponto. O fato de que o entrelaçador possui fatores de espalhamento (s, t) é refletido no fato de que cada quadrilátero contém apenas o ponto em seu centro e mais nenhum outro.

Definição 4.7 (Parâmetro s) *Define-se o parâmetro s de um entrelaçador como o valor máximo de s que satisfaz a desigualdade $s \leq t$.*

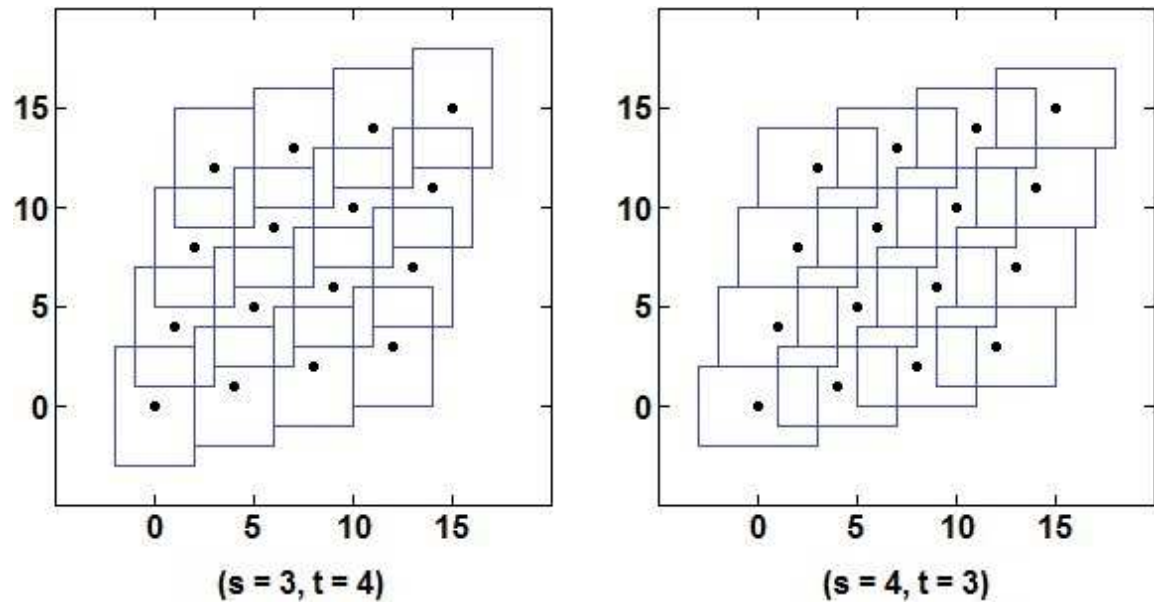


Figura 4.2: Espalhamentos do entrelaçador LRTB de ordem 4.

No caso ilustrado pela Figura 4.2, o parâmetro s do entrelaçador é 3. Quando $s = 1$, diz-se que o entrelaçador possui um fator de espalhamento trivial.

Definição 4.8 (Espalhamento normalizado) O parâmetro de espalhamento normalizado de um entrelaçador, denotado por λ , é definido como

$$\lambda = \frac{2s}{T}. \quad (4.7)$$

O espalhamento normalizado de um entrelaçador assume valores no intervalo $[0, 1]$.

4.4 Alguns Entrelaçadores Paramétricos

Nesta seção são apresentados alguns entrelaçadores paramétricos considerados nesta tese para serem aplicados nos esquemas propostos de codificação homofônica universal. São apresentadas suas respectivas funções de permutação e algumas considerações sobre suas dispersões e espalhamento.

4.4.1 O Entrelaçador de Berrou-Glavieux (BGL)

O entrelaçador de Berrou-Glavieux [13, 14] consiste em uma matriz $N \times M$, em que $N = 2^n$, $M = 2^m$, com $n \geq 3$. O período desse entrelaçador é $T = N \cdot M$. Para $0 \leq i < T$, a função de permutação $\pi(i)$ é definida como

$$\pi(i) = r(i)M + c(i), \quad (4.8)$$

em que

$$\begin{aligned} c_o &\equiv i \pmod{M}, \\ r_o &= \frac{i - c_o}{M}, \\ l &\equiv r_o + c_o \pmod{8}, \\ c(i) &\equiv p(l)(c_o + 1) - 1 \pmod{M}, \\ r(i) &\equiv \left(\frac{N}{2} + 1\right)(r_o + c_o) \pmod{N}. \end{aligned}$$

Os números $p(j)$, $0 \leq j \leq 7$, são relativamente primos com M e N e são apresentados na Tabela 4.1.

Tabela 4.1: Números primos definidos para o entrelaçador de Berrou-Glavieux.

j	0	1	2	3	4	5	6	7
$p(j)$	17	37	19	29	41	23	13	7

Segundo [14], o fator multiplicativo $\left(\frac{N}{2} + 1\right)$ é usado para evitar que símbolos vizinhos na leitura sejam escritos em linhas consecutivas. Quando $M = N$, diz-se que o entrelaçador possui ordem N .

Dispersão do Entrelaçador de Berrou-Glavieux

As Figuras 4.3 e 4.4 ilustram as dispersões do entrelaçador de Berrou-Glavieux, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz). Observando esses gráficos, percebe-se, para os períodos considerados, que as curvas de dispersão são semelhantes, em que o maior valor de dispersão ocorre quando $N = 8$ (entre 0,35 e 0,4), decrescendo à medida que o valor de N cresce. Para um determinado valor de N , quanto maior for o valor de T , menor é o valor da dispersão nesse ponto.

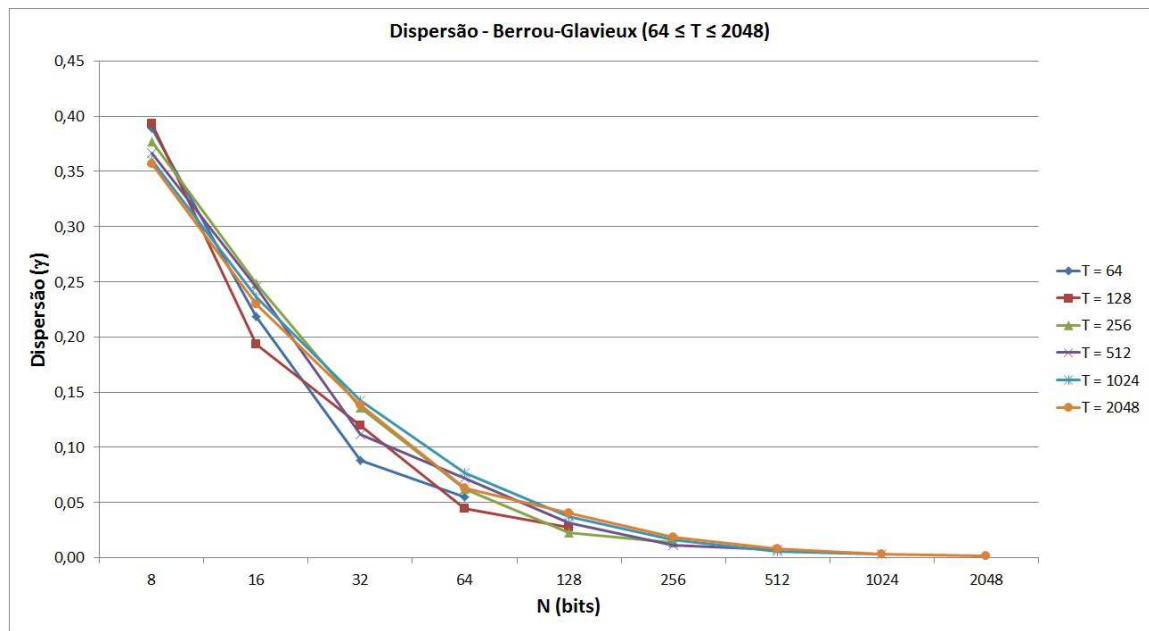


Figura 4.3: Dispersão do entrelaçador de Berrou-Glavieux para $64 \leq T \leq 2048$.

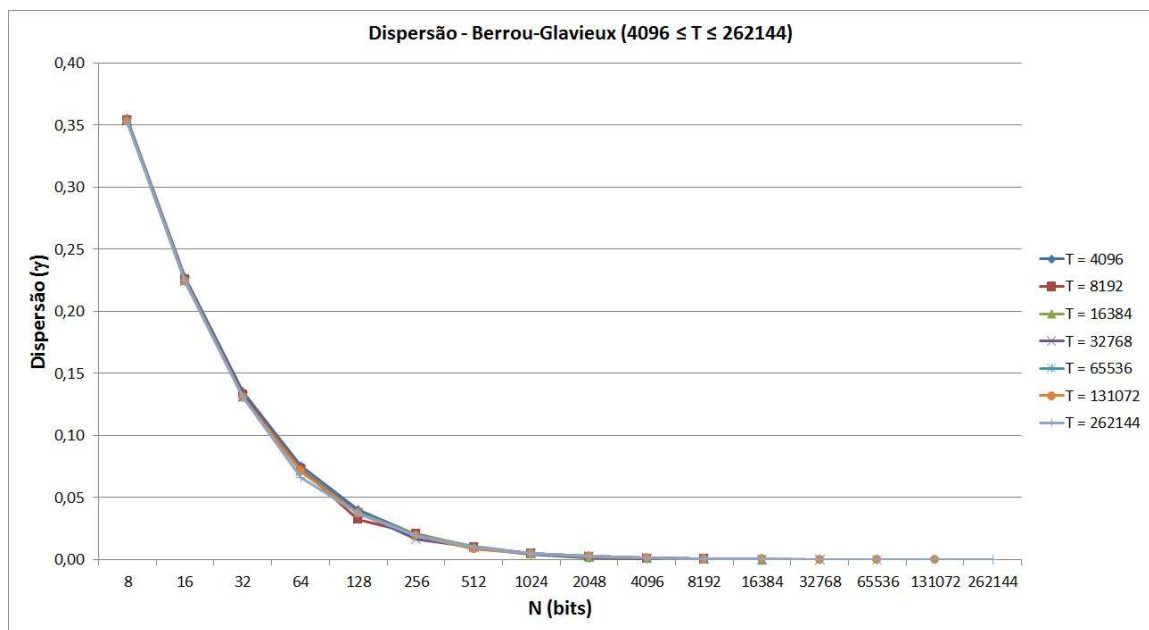


Figura 4.4: Dispersão do entrelaçador de Berrou-Glavieux para $4096 \leq T \leq 262144$.

Supondo $T = 2^k$ e $N = 2^n$, em que $3 \leq n \leq k$, é possível calcular analiticamente a dispersão e a dispersão normalizada do entrelaçador de Berrou-Glavieux para $\left\lfloor \frac{k}{2} \right\rfloor$ valores de n : $k+1 - \left\lfloor \frac{k}{2} \right\rfloor \leq n \leq k$. Para cada um dos valores de n no intervalo, a dispersão é uma função afim em relação a T . A Tabela 4.2 apresenta as expressões analíticas para a dispersão e para a dispersão normalizada. São apresentados os valores de k em que cada uma das fórmulas é

aplicável, considerando $6 \leq k \leq 18$.

Tabela 4.2: Expressões analíticas para a dispersão e para a dispersão normalizada do entrelaçador de Berrou-Glavieux.

n	Γ	γ	k
k	$\frac{7T-8}{4}$	$\frac{7T-8}{2T(T-1)}$	$6 \leq k \leq 18$
$k-1$	$\frac{23T-56}{8}$	$\frac{23T-56}{4T(T-1)}$	$6 \leq k \leq 18$
$k-2$	$\frac{529T-5632}{64}$	$\frac{529T-5632}{32T(T-1)}$	$6 \leq k \leq 18$
$k-3$	$\frac{1239T-33344}{64}$	$\frac{1239T-33344}{32T(T-1)}$	$8 \leq k \leq 18$
$k-4$	$\frac{682T-52800}{16}$	$\frac{682T-52800}{8T(T-1)}$	$10 \leq k \leq 18$
$k-5$	$\frac{22313T-4644608}{256}$	$\frac{22313T-4644608}{128T(T-1)}$	$12 \leq k \leq 18$
$k-6$	$\frac{21893T-12783744}{128}$	$\frac{21893T-12783744}{64T(T-1)}$	$14 \leq k \leq 18$
$k-7$	$\frac{172611T-318688768}{512}$	$\frac{172611T-318688768}{256T(T-1)}$	$16 \leq k \leq 18$

Exemplo 4.1 Considere $T = 256 = 2^8$. As dispersões associadas aos $\left\lfloor \frac{k}{2} \right\rfloor = 4$ valores de n , em que $5 \leq n \leq 8$ são as seguintes:

$$\begin{aligned}
 N = 2^8 = 256 &\rightarrow \Gamma = \frac{7 \cdot 256 - 8}{4} = 446, \\
 N = 2^7 = 128 &\rightarrow \Gamma = \frac{23 \cdot 256 - 56}{8} = 729, \\
 N = 2^6 = 64 &\rightarrow \Gamma = \frac{529 \cdot 256 - 5632}{64} = 2028, \\
 N = 2^5 = 32 &\rightarrow \Gamma = \frac{1239 \cdot 256 - 33344}{64} = 4435.
 \end{aligned}$$

Espalhamento do Entrelaçador de Berrou-Glavieux

As Figuras 4.5 e 4.6 ilustram o fator λ de espalhamento do entrelaçador de Berrou-Glavieux, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz). Observando esses gráficos, percebe-se, para todos os períodos considerados, que as curvas de espalhamento são semelhantes, porém com valores baixos bem próximos de zero. Para um determinado valor de N , quanto maior for o valor de T , menor é o valor do fator λ nesse ponto.

Em todos os períodos considerados, há até três pontos com maior espalhamento. O espalhamento associado a $N = 8$ se destaca apenas em alguns períodos, sendo o maior de todos apenas quando $T = 16384$. Supondo $T = 2^k$, se k for ímpar, o espalhamento associado a $N = 2^{\lfloor \frac{k}{2} \rfloor + 1}$ é o maior de todos, enquanto que se k for par, os espalhamentos associados a $N = 2^{\lfloor \frac{k}{2} \rfloor}$ e $N = 2^{\lfloor \frac{k}{2} \rfloor + 1}$ são os que mais se destacam, sendo o espalhamento associado a $N = 2^{\lfloor \frac{k}{2} \rfloor + 1}$ o maior.

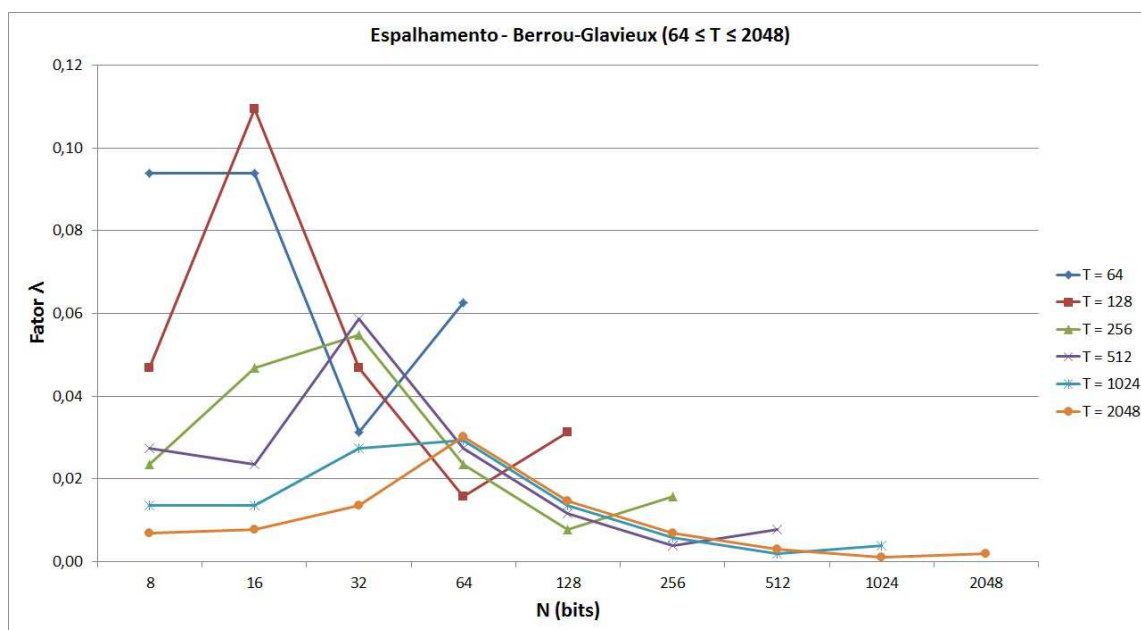


Figura 4.5: Fator λ (espalhamento) do entrelaçador de Berrou-Glavieux para $64 \leq T \leq 2048$.

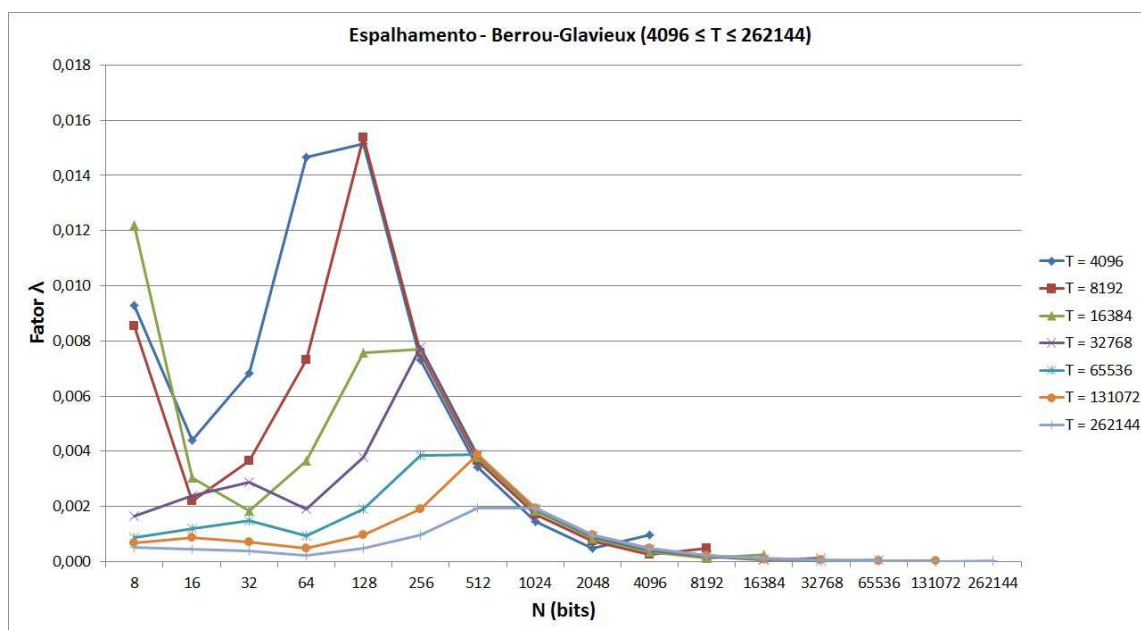


Figura 4.6: Fator λ (espalhamento) do entrelaçador de Berrou-Glavieux para $4096 \leq T \leq 262144$.

Supondo $T = 2^k$ e $N = 2^n$, em que $3 \leq n \leq k$, é possível calcular analiticamente o parâmetro s e o fator λ do entrelaçador de Berrou-Glavieux para $k - \left\lfloor \frac{k}{2} \right\rfloor$ valores de n :

$\lfloor \frac{k}{2} \rfloor + 1 \leq n \leq k$. Nesse intervalo, parâmetro s é expresso como

$$s = \begin{cases} 2^{n-1} - 2, & \text{se } n = \lfloor \frac{k}{2} \rfloor \quad (8 \leq k \leq 18) \\ 2^{k-n} - 1, & \text{se } \lfloor \frac{k}{2} \rfloor + 1 \leq n \leq k + 1 \\ 2, & \text{se } n = k. \end{cases} \quad (4.9)$$

Conseqüentemente, o fator λ é expresso como

$$\lambda = \begin{cases} 2^{n-k} - 2^{2-k}, & \text{se } n = \lfloor \frac{k}{2} \rfloor \quad (8 \leq k \leq 18) \\ 2^{1-n} - 2^{1-k}, & \text{se } \lfloor \frac{k}{2} \rfloor + 1 \leq n \leq k + 1 \\ 2^{2-k}, & \text{se } n = k. \end{cases} \quad (4.10)$$

4.4.2 O Entrelaçador JPL

O entrelaçador JPL foi desenvolvido no *Jet Propulsion Laboratory* da NASA e foi sugerido para ser utilizado no padrão CCSDS (*Consultative Committee for Space Data Systems*) [15]. Ele consiste em uma matriz $N \times M$ em que N é par. O período desse entrelaçador é $T = N \cdot M$. Para $0 \leq i < T$, a função de permutação $\pi(i)$ é definida como

$$\pi(i) = 2r(i) + Nc(i) - m(i) + 1, \quad (4.11)$$

em que

$$\begin{aligned} m(i) &\equiv i \pmod{2}, \\ c_o &\equiv \frac{i - m(i)}{2} \pmod{M}, \\ r_o &= \frac{\frac{i - m(i)}{2} - c_o}{M}, \\ r(i) &\equiv 19r_o + 1 \pmod{\frac{N}{2}}, \\ l &\equiv r(i) \pmod{8}, \\ c(i) &\equiv p(l)c_o + 21m \pmod{M}. \end{aligned}$$

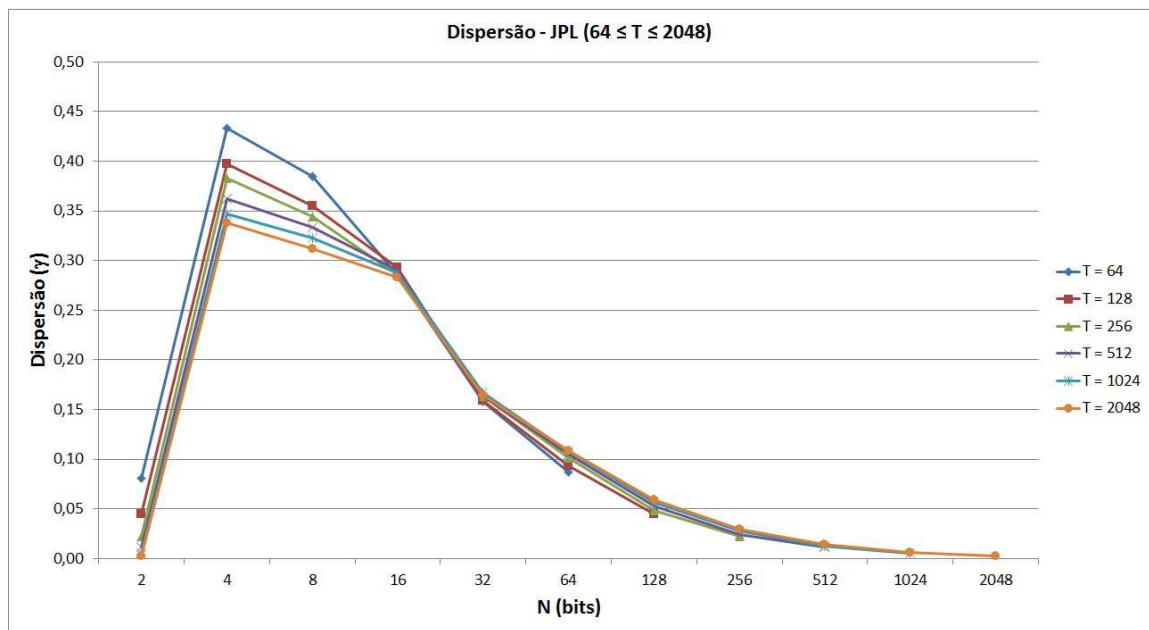
Os números $p(j)$, $0 \leq j \leq 7$, são relativamente primos com M e N e são apresentados na Tabela 4.3.

Tabela 4.3: Números primos definidos para o entrelaçador JPL.

j	0	1	2	3	4	5	6	7
$p(j)$	31	37	43	47	53	59	61	67

Dispersão do Entrelaçador JPL

As Figuras 4.7 e 4.8 ilustram as dispersões do entrelaçador JPL, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz). Observando esses gráficos, percebe-se, para os períodos considerados, que as curvas de dispersão são semelhantes, em que o maior valor de dispersão ocorre quando $N = 4$ (entre 0,3 e 0,45), decrescendo à medida que o valor de N cresce. Para um determinado valor de N , quanto maior for o valor de T , menor é o valor da dispersão nesse ponto.

Figura 4.7: Dispersão do entrelaçador JPL para $64 \leq T \leq 2048$.

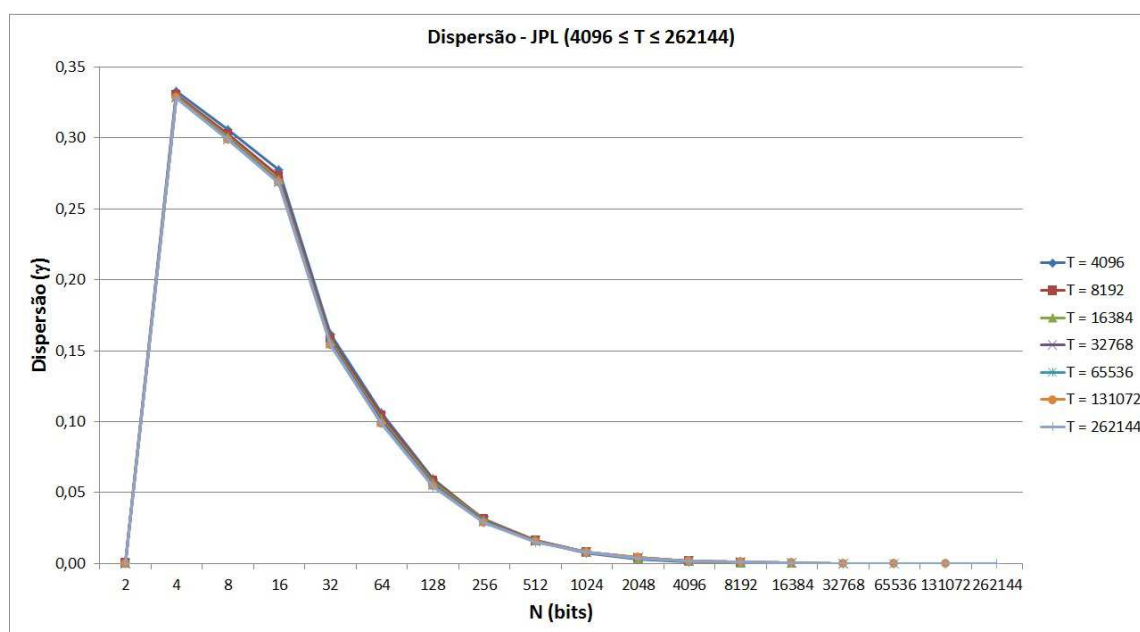


Figura 4.8: Dispersão do entrelaçador JPL para $4096 \leq T \leq 262144$.

Espalhamento do Entrelaçador JPL

As Figuras 4.9 e 4.10 ilustram o fator λ de espalhamento do entrelaçador JPL, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz). Observando esses gráficos, percebe-se, para todos os períodos considerados, que as curvas de espalhamento são semelhantes, porém com valores baixos bem próximos de zero. O maior valor de espalhamento ocorre quando $N = 2$ (a única exceção é quando $T = 128$), decrescendo à medida que o valor de N cresce. Quando $N = 2$, o valor do fator λ permanece praticamente constante à medida que o valor de T cresce.

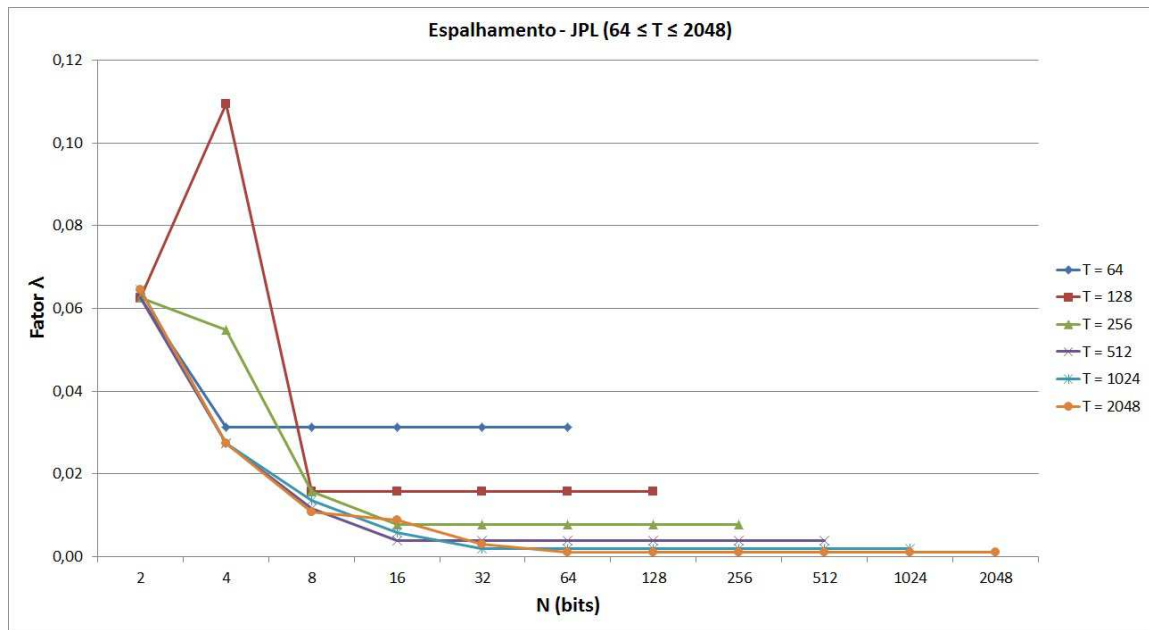


Figura 4.9: Fator λ (espalhamento) do entrelaçador JPL para $64 \leq T \leq 2048$.

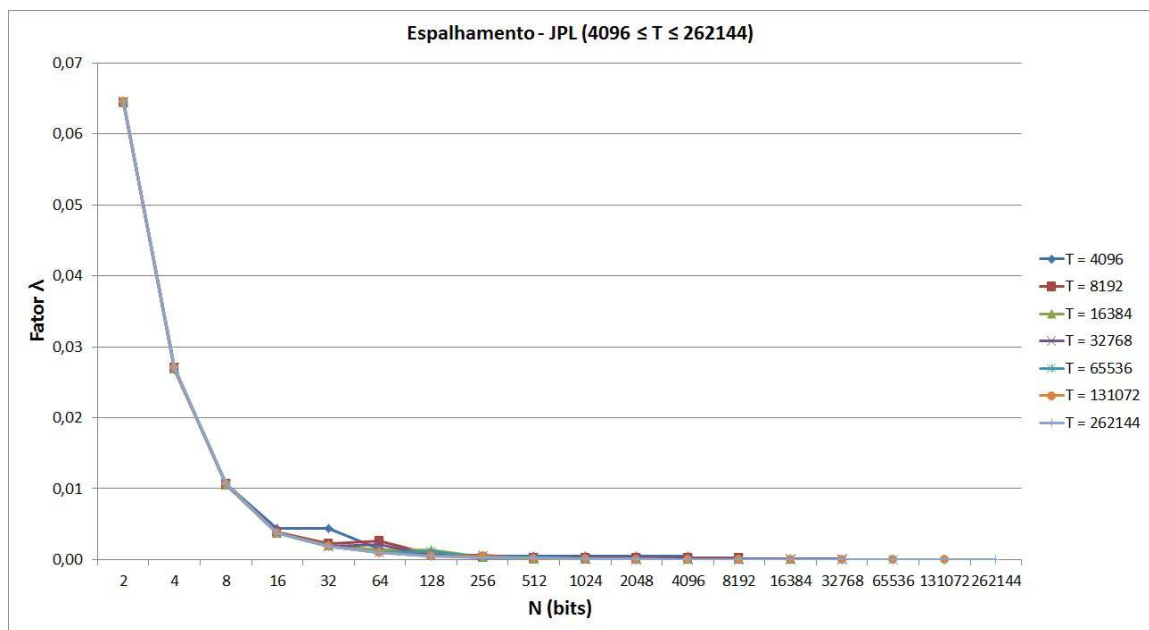


Figura 4.10: Fator λ (espalhamento) do entrelaçador JPL para $4096 \leq T \leq 262144$.

Supondo $T = 2^k$ e $N = 2^n$, fazendo $w = \left\lfloor \frac{k}{5} \right\rfloor$, pode-se expressar analiticamente o parâmetro s como

$$s = \begin{cases} \sum_{i=1}^w 2^{k-5i}, & \text{se } n = 1 \\ 1, & \text{se } n \geq k - 5 \quad (k \geq 9). \end{cases} \quad (4.12)$$

Conseqüentemente, o fator λ é expresso como

$$\lambda = \begin{cases} \sum_{i=1}^w 2^{1-5i}, & \text{se } n = 1 \\ 2^{1-k}, & \text{se } n \geq k - 5 \text{ (} k \geq 9 \text{)}. \end{cases} \quad (4.13)$$

Exemplo 4.2 *Suponha $T = 65536 = 2^{16}$. Nesse caso, tem-se $w = \left\lfloor \frac{k}{5} \right\rfloor = \left\lfloor \frac{13}{5} \right\rfloor = 3$. Então, para $N = 2$ (espalhamento máximo) o parâmetro s é calculado como*

$$s = \sum_{i=1}^3 2^{16-5i} = 2^{11} + 2^6 + 2^1 = 2114.$$

O fator λ é calculado como

$$\lambda = \sum_{i=1}^3 2^{1-5i} = 2^{-4} + 2^{-9} + 2^{-14} = 0,064514.$$

Para $N \geq 2048$, tem-se $s = 1$ e $\lambda = 0,000031$.

4.4.3 Os Entrelaçadores Clássicos de Bloco

Os entrelaçadores clássicos de bloco são definidos como uma matriz $N \times M$, em que os símbolos são escritos nas linhas e lidos através das colunas [21]. O período desse entrelaçador é $T = N \times M$. Existem quatro tipos de entrelaçadores clássicos de bloco, em função da ordem de leitura dos símbolos:

LRTB (*Left-Right Top-Bottom*): Leitura nas colunas da esquerda para a direita e de cima para baixo;

LRBT (*Left-Right Bottom-Top*): Leitura nas colunas da esquerda para a direita e de baixo para cima;

RLTB (*Right-Left Top-Bottom*): Leitura nas colunas da direita para a esquerda e de cima para baixo;

RLBT (*Right-Left Bottom-Top*): Leitura nas colunas da direita para a esquerda e de baixo para cima.

A função de permutação para cada um desses entrelaçadores é definida como

LRTB:

$$\pi(i) = Mi \pmod{T-1}, \quad 0 \leq i < T-1, \quad (4.14)$$

$$\pi(T-1) = T-1. \quad (4.15)$$

LRBT:

$$\pi(i) = (N-1-i)M \pmod{T+1}, \quad 0 \leq i < T. \quad (4.16)$$

RLTB:

$$\pi(i) = (i+1)M-1 \pmod{T+1}, \quad 0 \leq i < T. \quad (4.17)$$

RLBT:

$$\pi(0) = T-1, \quad (4.18)$$

$$\pi(i) = (N-i)M-1 \pmod{T-1}, \quad 1 \leq i < T. \quad (4.19)$$

Dispersão dos Entrelaçadores Clássicos de Bloco

Os entrelaçadores LRBT, LRTB, RLBT e RLTB possuem a mesma dispersão para um dado período, ou seja, suas curvas de dispersão são iguais. As Figuras 4.11 e 4.12 ilustram a dispersão dos entrelaçadores clássicos de bloco, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz). Observando esses gráficos, percebe-se, para todos os períodos considerados, que as curvas de dispersão são semelhantes.

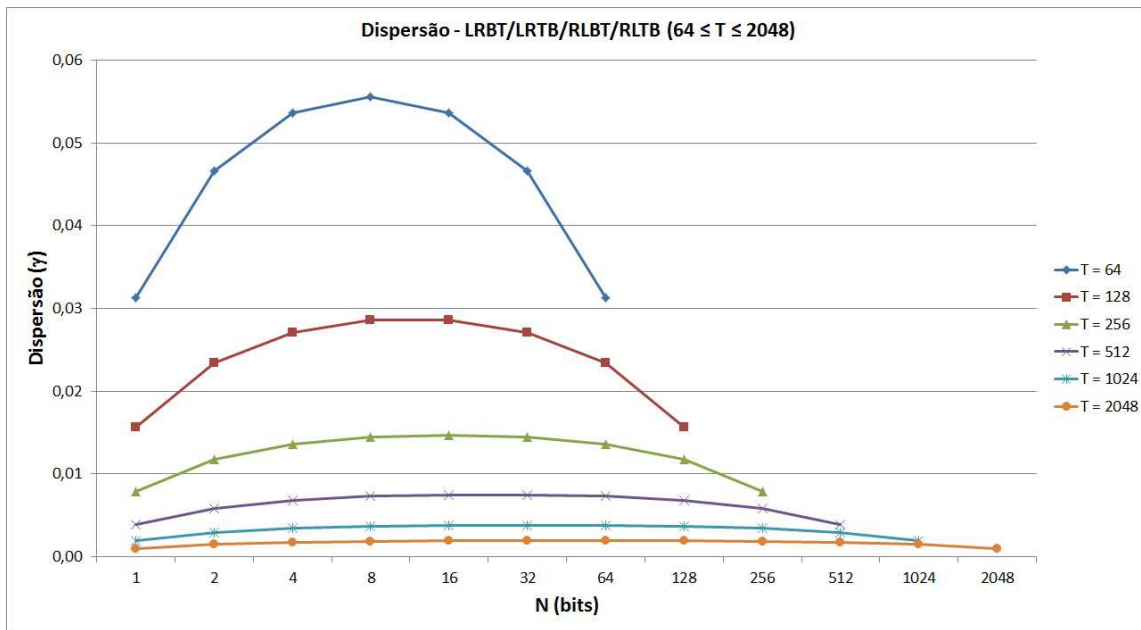


Figura 4.11: Dispersão dos entrelaçadores clássicos de bloco para $64 \leq T \leq 2048$.

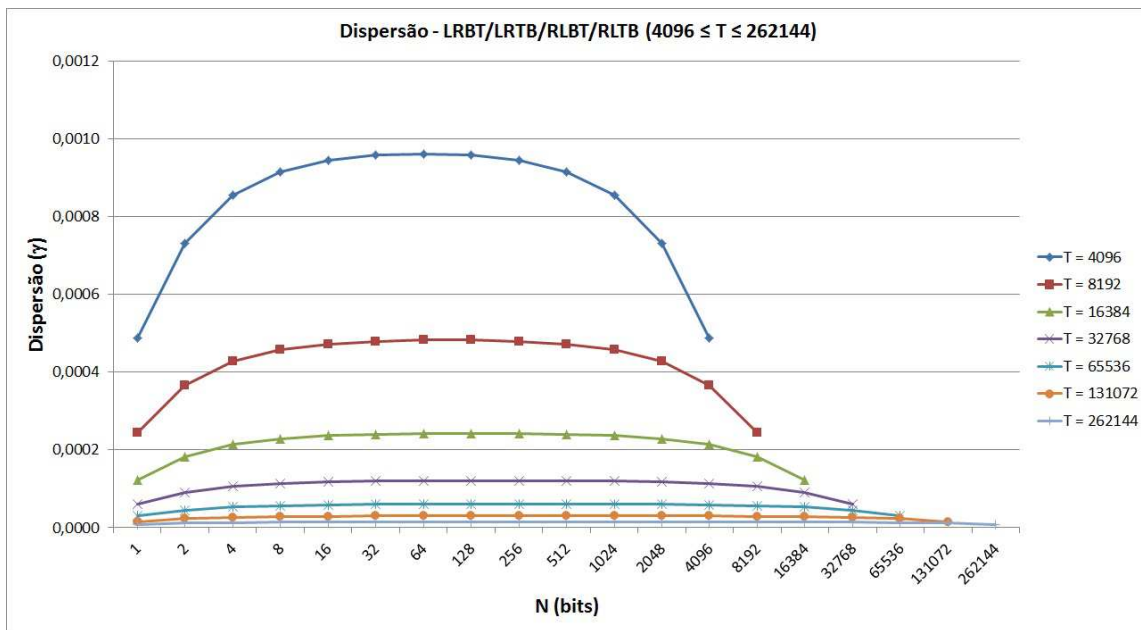


Figura 4.12: Dispersão dos entrelaçadores clássicos de bloco para $4096 \leq T \leq 262144$.

A expressão analítica para a dispersão dos entrelaçadores clássicos de bloco é

$$\Gamma = 2NM - N - M. \tag{4.20}$$

A expressão analítica para a dispersão normalizada dos entrelaçadores clássicos de bloco

é

$$\gamma = \frac{4MN - 2N - 2M}{(MN)^2 - MN} = \frac{4NT - 2N^2 - 2T}{N(T^2 - T)}. \quad (4.21)$$

Fazendo $\frac{\partial \gamma}{\partial N} = 0$, conclui-se que a dispersão é máxima quando $N = \sqrt{T}$, o que pode ser notado observando as Figuras 4.11 e 4.12. Para um determinado valor de N , a dispersão decresce à medida que o período do entrelaçador cresce. As dispersões associadas aos entrelaçadores clássicos de bloco são baixas, sendo menores que 0,06.

Espalhamento dos Entrelaçadores Clássicos de Bloco

Os entrelaçadores LRBT, LRTB, RLBT e RLTB possuem praticamente o mesmo fator λ para um dado período, ou seja, suas curvas de espalhamento são aproximadamente iguais. As Figuras 4.13 e 4.14 ilustram o fator λ de espalhamento dos entrelaçadores LRBT e RLTB, considerando o período $T = 2^k$, em que $6 \leq k \leq 18$. O eixo das abscissas representa o parâmetro N em *bits* (a quantidade de linhas da matriz).

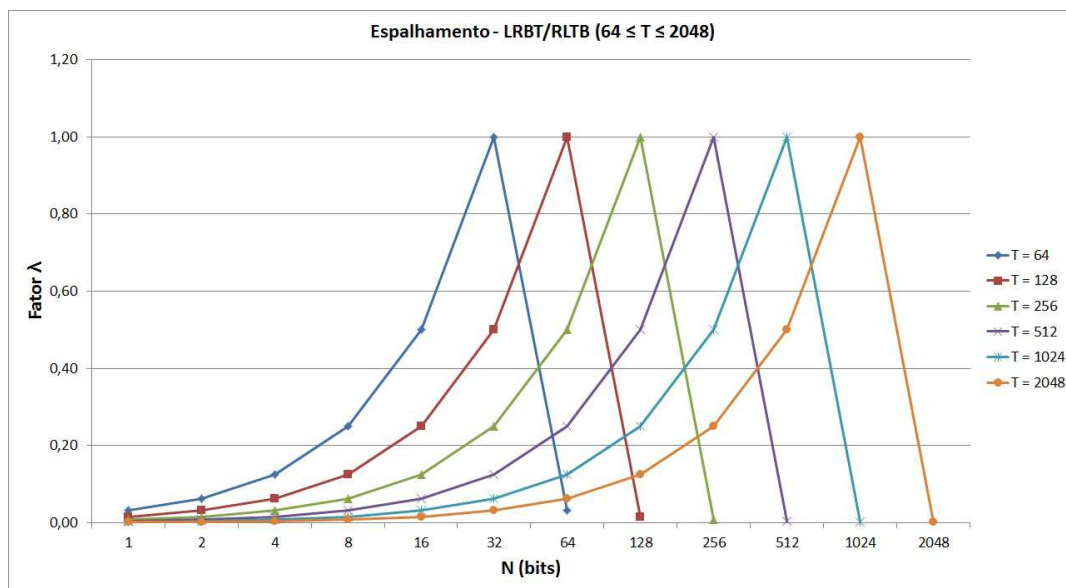


Figura 4.13: Fator λ (espalhamento) dos entrelaçadores LRBT e RLTB para $64 \leq T \leq 2048$.

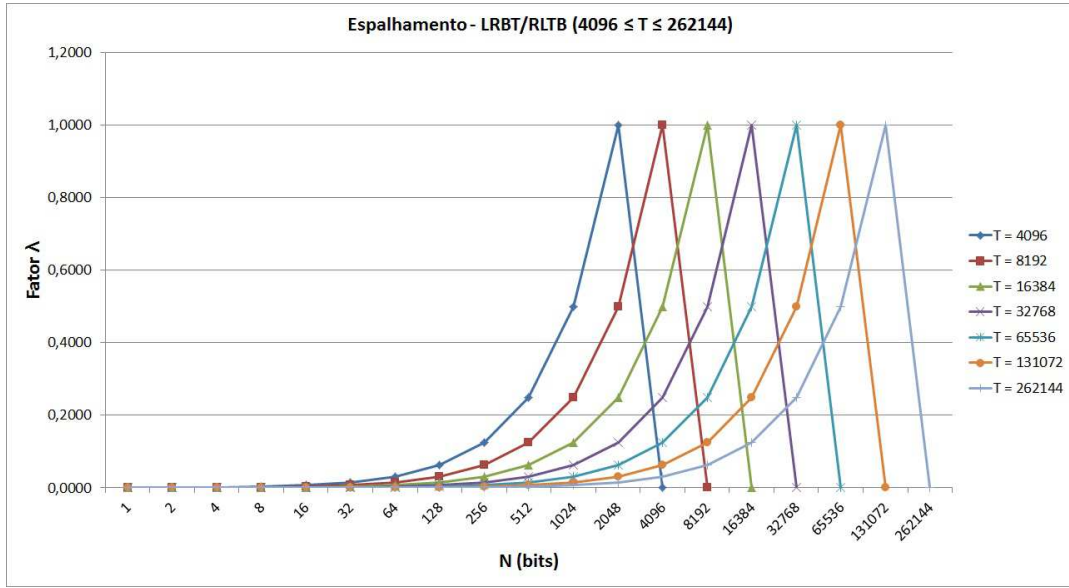


Figura 4.14: Fator λ (espalhamento) dos entrelaçadores LRBT e RLTB para $4096 \leq T \leq 262144$.

Observando esses gráficos, percebe-se que, para todos os períodos considerados, as curvas de espalhamento são semelhantes. O espalhamento cresce à medida que o valor de N cresce, até chegar em seu valor máximo, que ocorre quando $N = \frac{T}{2}$. Quando $N = T$, tem-se $s = 1$, o que implica em λ muito próximo de zero.

Supondo $T = 2^k$ e $N = 2^n$, as expressões analíticas para o parâmetro s e para o fator λ dos entrelaçadores LRBT e RLTB são

$$s = \begin{cases} 2^n, & \text{se } n \neq k \\ 1, & \text{se } n = k, \end{cases} \quad (4.22)$$

$$\lambda = \begin{cases} 2^{n-k+1}, & \text{se } n \neq k \\ 2^{1-k}, & \text{se } n = k. \end{cases} \quad (4.23)$$

As expressões analíticas para o parâmetro s e para o fator λ dos entrelaçadores LRBT e RLTB são

$$s = \begin{cases} 2^n, & \text{se } n \leq \lfloor \frac{k+1}{2} \rfloor - 1 \\ 2^n - 1, & \text{se } \lfloor \frac{k+1}{2} \rfloor \leq n \leq k - 1 \\ 1, & \text{se } n = k, \end{cases} \quad (4.24)$$

$$\lambda = \begin{cases} 2^{n-k+1}, & \text{se } n \leq \lfloor \frac{k+1}{2} \rfloor - 1 \\ 2^{n-k+1} - 2^{1-k}, & \text{se } \lfloor \frac{k+1}{2} \rfloor \leq n \leq k - 1 \\ 2^{1-k}, & \text{se } n = k. \end{cases} \quad (4.25)$$

4.4.4 O Entrelaçador Co-Primo (CPR)

O entrelaçador co-primo consiste em um vetor de comprimento T (período do entrelaçador). Escolhe-se duas constantes a e b , em que $0 < a < T$, $0 \leq b < T$ e $\text{mdc}(a, T) = 1$ [21]. Para $0 \leq i < T$, a função de permutação $\pi(i)$ é definida como

$$\pi(i) = ai + b \pmod{T}. \quad (4.26)$$

Dispersão do Entrelaçador Co-Primo

A Figura 4.15 ilustra a dispersão do entrelaçador Co-Primo, considerando os períodos e parâmetros apresentados na Tabela 4.4, em que o eixo das abscissas representa os parâmetros T , a e b do entrelaçador.

Tabela 4.4: Parâmetros considerados para o entrelaçador Co-Primo.

T	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144
a	3	13	19	23	5	7	11	29	41	43	761	61	71
b	16	25	64	102	256	409	44	1638	4096	6553	87	26214	65536

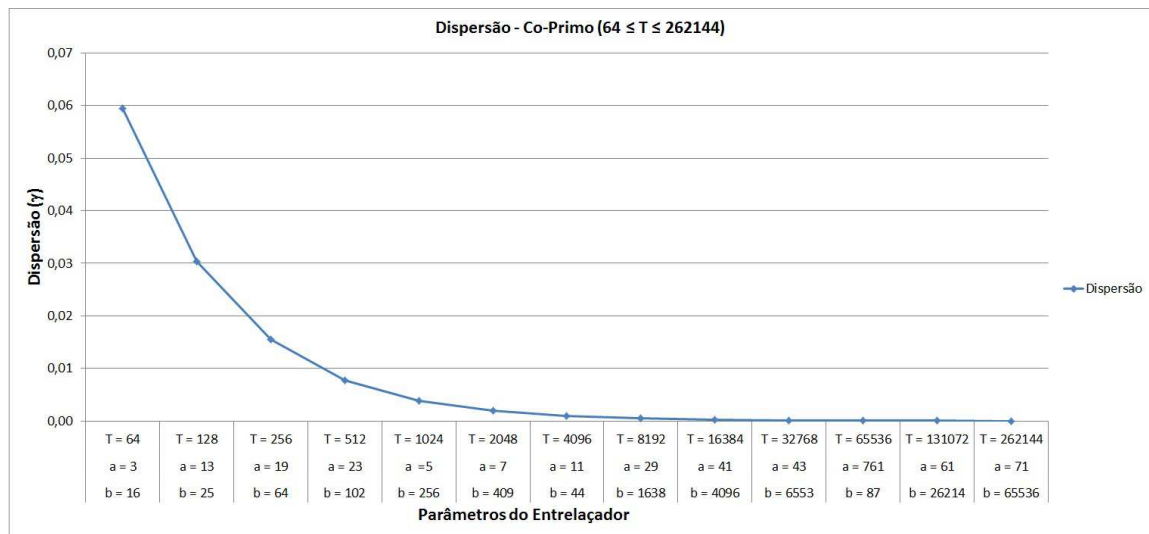


Figura 4.15: Dispersão do entrelaçador Co-Primo para $64 \leq T \leq 262144$.

Observando esse gráfico, percebe-se que o maior valor da dispersão ocorre quando $T = 64$, $a = 3$ e $b = 16$, decrescendo à medida que o período do entrelaçador cresce. Essas dispersões são baixas, sendo menores do que 0,06. Considerando $T = 2^k$, em que $6 \leq k \leq 18$, uma expressão para o valor aproximado da dispersão do entrelaçador Co-Primo é

$$\Gamma \approx 2^{k+1}. \quad (4.27)$$

Assim, a expressão aproximada para a dispersão normalizada do entrelaçador Co-Primo é

$$\gamma \approx \frac{4}{2^k - 1}. \quad (4.28)$$

Essas aproximações possuem um erro médio de 2,5% nos períodos considerados. Considerando um período T constante, não há alterações significativas no valor da dispersão do entrelaçador variando-se os parâmetros a e b .

Espalhamento do Entrelaçador Co-Primo

Considerando um período T fixo, o parâmetro s do entrelaçador Co-Primo só sofre influência do parâmetro a , ou seja, se esse parâmetro for constante, o parâmetro s é o mesmo para qualquer valor considerado de b . Considerando $T \leq 128$, a curva do parâmetro s em função de a é bem característica e possui o mesmo formato, variando-se o valor de T . A Figura 4.16 ilustra essa curva quando $T = 256$. O eixo das abscissas representa o parâmetro a do entrelaçador.

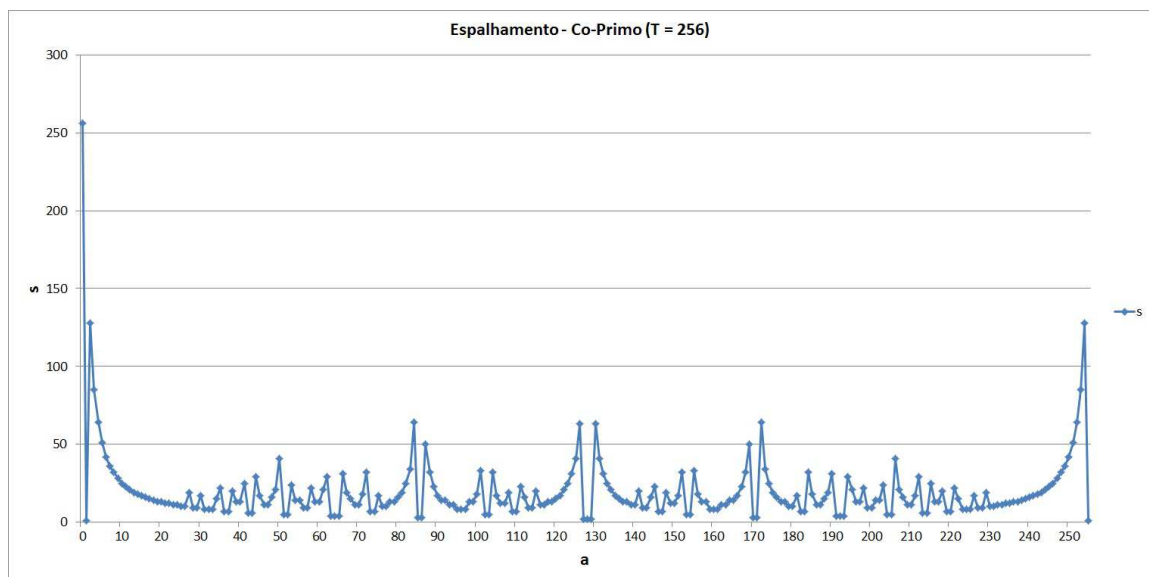


Figura 4.16: Parâmetro s do entrelaçador Co-Primo quando $T = 256$.

Observando esse gráfico, nota-se que existem três pontos onde o parâmetro s atinge o maior valor: quando $a = 0$ ($s = T = 256$), quando $a = 2$ ($s = \frac{T}{2} = 128$) e quando $a = T - 2 = 254$ ($s = \frac{T}{2} = 128$). Além disso, observa-se $s = 1$ quando $a = 1$ e $s = 2$ quando $a = \frac{T}{2} - 1$, quando $a = \frac{T}{2}$ e quando $a = \frac{T}{2} + 1$.

A Tabela 4.5 apresenta os três pontos em que o parâmetro s e o fator λ atingem o maior

valor e os quatro pontos em que atingem o menor valor, em função do período T . Os pontos citados nessa tabela estão presentes para $T \geq 128$.

Tabela 4.5: Pontos máximos e mínimos da curva do parâmetro s do entrelaçador Co-Primo.

	a	s	λ
Pontos Máximos	0	T	2
	2	$\frac{T}{2}$	1
	$T - 2$	$\frac{T}{2}$	1
Pontos Mínimos	1	1	$\frac{2}{T}$
	$\frac{T}{2} - 1$	2	$\frac{4}{T}$
	$\frac{T}{2}$	2	$\frac{4}{T}$
	$\frac{T}{2} + 1$	2	$\frac{4}{T}$

4.4.5 O Entrelaçador de Takeshita-Costello (TKC)

O entrelaçador de Takeshita-Costello [16] consiste em um vetor de comprimento T (período do entrelaçador). Define-se uma constante k ímpar tal que $0 < k < T$ e outra constante h , tal que $0 \leq h < T$. Para $0 \leq i < T$, a função de permutação $\pi(i)$ é definida como

$$\pi(c(T-1) - h \pmod{T}) = c(0), \quad (4.29)$$

$$\pi(c(i-1) - h \pmod{T}) = c(i), \quad (4.30)$$

em que $c(i) = \frac{ki(i+1)}{2} \pmod{T}$.

Dispersão do Entrelaçador de Takeshita-Costello

A Figura 4.17 ilustra a dispersão do entrelaçador de Takeshita-Costello, considerando os períodos e parâmetros apresentados na Tabela 4.6, em que o eixo das abscissas representa os parâmetros T , k e h do entrelaçador.

Tabela 4.6: Parâmetros considerados para o entrelaçador de Takeshita-Costello.

T	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144
k	3	13	19	23	5	7	11	29	41	43	761	61	71
h	16	25	64	102	256	409	44	1638	4096	6553	87	26214	65536

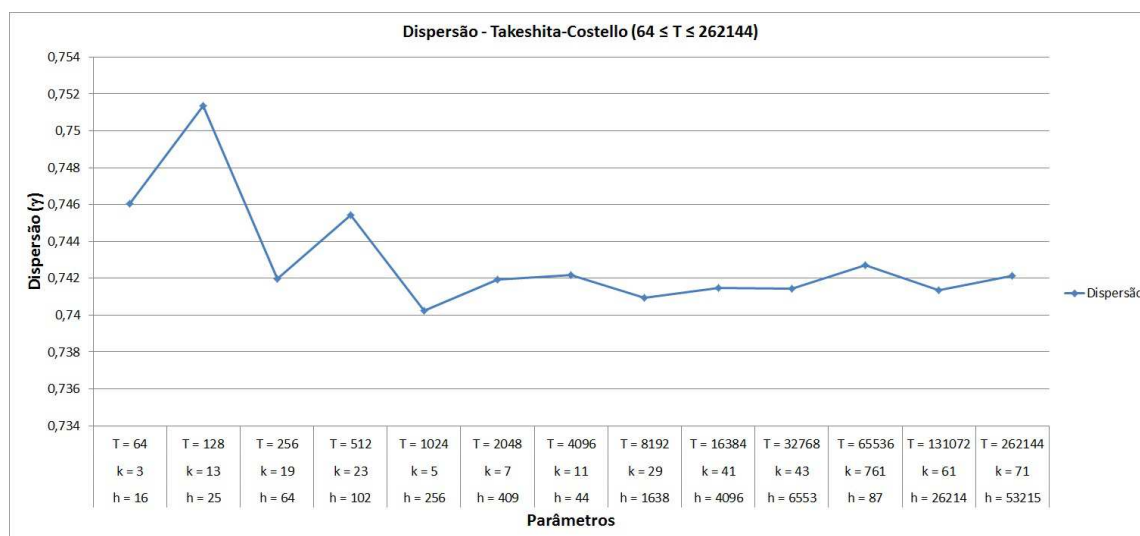


Figura 4.17: Dispersão do entrelaçador de Takeshita-Costello para $64 \leq T \leq 262144$.

Observando esse gráfico, percebe-se, para os períodos e parâmetros considerados, que esse entrelaçador possui uma dispersão alta entre aproximadamente 0,74 e 0,752. Considerando um período T constante, não há alterações significativas no valor da dispersão do entrelaçador variando-se os parâmetros k e h .

Espalhamento do Entrelaçador de Takeshita-Costello

O entrelaçador de Takeshita-Costello possui apenas fatores triviais de espalhamento, ou seja, $s = 1$ para qualquer período e parâmetros considerados [21]. Conseqüentemente, tem-se que $\lambda = \frac{2}{T}$ decresce à medida que T cresce. A Figura 4.18 ilustra o fator λ do entrelaçador de Takeshita-Costello, considerando os períodos e parâmetros apresentados na Tabela 4.6, em que o eixo das abscissas representa os parâmetros T , a e b do entrelaçador.

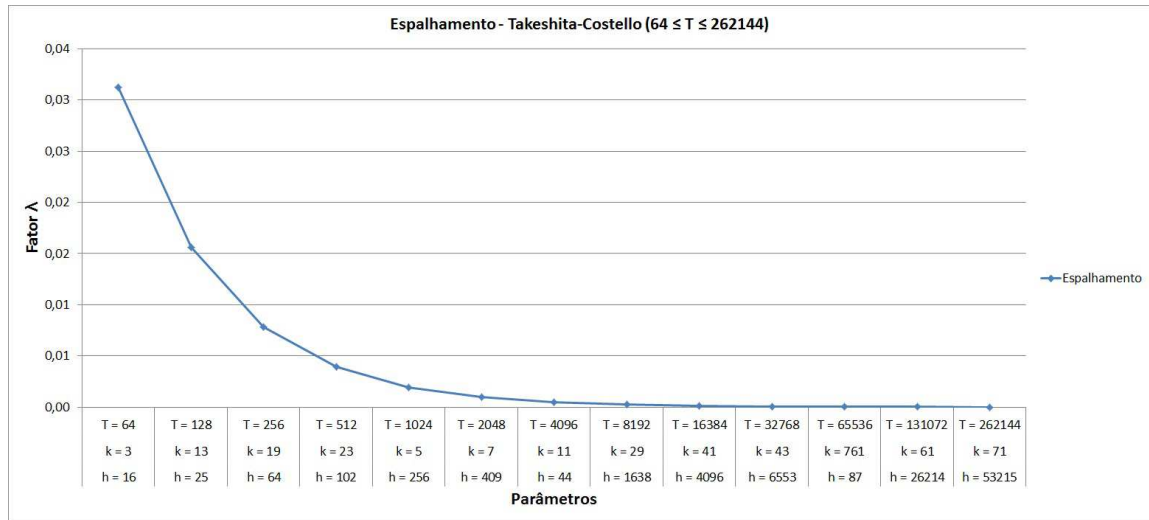


Figura 4.18: Fator λ (espalhamento) do entrelaçador de Takeshita-Costello para $64 \leq T \leq 262144$.

4.4.6 O Entrelaçador de Welch-Costas

O entrelaçador de Welch-Costas [17] consiste em um vetor de comprimento $T = p - 1$ (período do entrelaçador), em que p é um número primo. Seja α uma raiz primitiva módulo p . Para $0 \leq i < T$, a função de permutação $\pi(i)$ é definida como

$$\pi(i) = \alpha^i - 1 \pmod{T + 1}. \quad (4.31)$$

Dispersão do Entrelaçador de Welch-Costas (WLC)

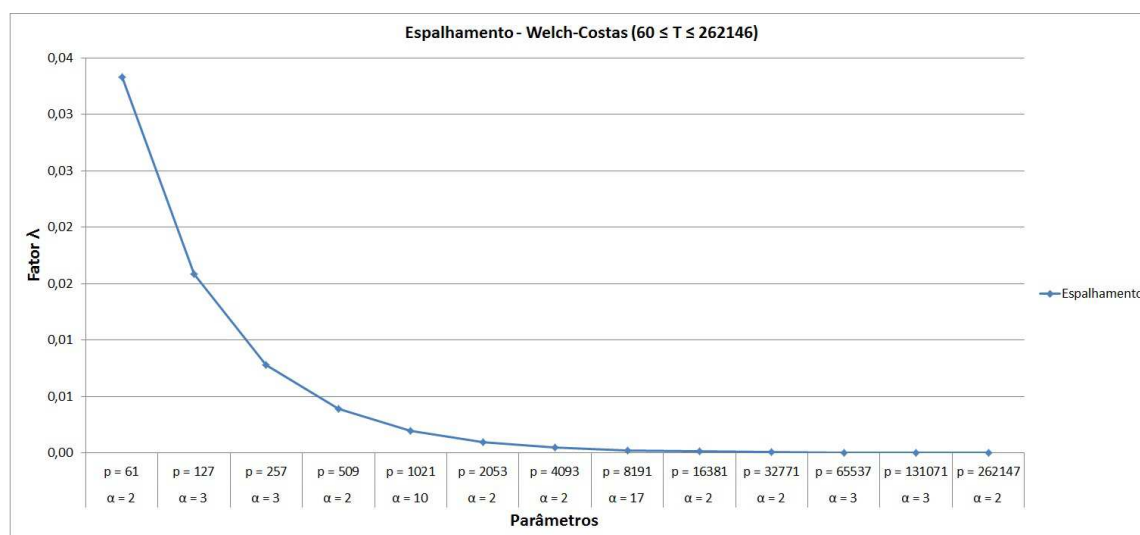
O entrelaçador de Welch-Costas possui dispersão máxima, ou seja, $\gamma = 1$ para qualquer T e α considerados [21].

Espalhamento do Entrelaçador de Welch-Costas

O entrelaçador de Welch-Costas possui apenas fatores triviais de espalhamento, ou seja, $s = 1$ para qualquer T e α considerados [21]. Conseqüentemente, tem-se que $\lambda = \frac{2}{T}$ decresce à medida que T cresce. A Figura 4.19 ilustra o fator λ do entrelaçador de Welch-Costas, considerando os períodos e parâmetros apresentados na Tabela 4.7, em que o eixo das abscissas representa esses parâmetros.

Tabela 4.7: Parâmetros considerados para o entrelaçador de Welch-Costas.

Caso	1	2	3	4	5	6	7	8	9	10	11	12	13
T	60	126	256	508	1020	2052	4092	8190	16380	32770	65536	131070	262146
p	61	127	257	509	1021	2053	4093	8191	16381	32771	65537	131071	262147
α	2	3	3	2	10	2	2	17	2	2	3	3	2

Figura 4.19: Fator λ (espalhamento) do entrelaçador de Welch-Costas para $60 \leq T \leq 262146$.

CAPÍTULO 5

AVALIAÇÕES DE ALEATORIEDADE

5.1 Introdução

A aleatoriedade de uma sequência binária é uma característica que desempenha um papel fundamental em aplicações criptográficas. Essa característica é desejável, por exemplo, em alguns sistemas como as cifras de fluxo, as funções hash e os codificadores homofônicos. Uma sequência binária aleatória pode ser interpretada como o resultado de lançamentos de uma moeda justa com faces numeradas com “0” e “1”, em que a probabilidade da ocorrência de cada face é $\frac{1}{2}$ em cada lançamento. Os lançamentos são independentes entre si, ou seja, nenhum resultado de lançamentos anteriores influencia o resultado de lançamentos futuros. Logo, o valor do próximo elemento da sequência não pode ser previsto a partir de elementos anteriores, independentemente do número de elementos já produzidos.

Tipicamente, a aleatoriedade de uma sequência binária é avaliada utilizando um ou mais testes estatísticos empíricos. Os testes são frequentemente agrupados em baterias (suítes) para permitir análises mais complexas de aleatoriedade. Existem diversos testes estatísticos possíveis, cada um avaliando a presença ou a falta de um padrão específico que, se detectado, pode indicar que a sequência não é aleatória. Devido a essa grande quantidade de testes, nenhum conjunto específico de testes pode ser considerado completo, pois sempre há a possibilidade de não ser considerado nesses testes algum aspecto de não-aleatoriedade. Assim, os resultados dos testes devem ser interpretados com cuidado para evitar conclusões incorretas sobre a sequência submetida. Existem cinco suítes bem conhecidas, utilizadas para análise

de aleatoriedade: a suíte de testes estatísticos do NIST [12], a suíte de testes Dieharder [45] (uma nova versão da bateria Diehard), a suíte de testes TestU01 [46], a suíte de testes ENT [47] e a suíte de testes CryptX [48].

Com relação aos testes realizados em sequências binárias, são feitas as seguintes suposições [12]:

Uniformidade: Em qualquer ponto de uma sequência binária aleatória ou pseudo-aleatória, a ocorrência de zeros e uns é igualmente provável (a probabilidade de ocorrência de cada um deles é $\frac{1}{2}$). O número esperado de zeros (ou uns) é $\frac{n}{2}$, em que n é o comprimento da sequência.

Escalabilidade: Qualquer teste aplicado a uma sequência pode também ser aplicado em subsequências extraídas de forma aleatória da sequência original. Se a sequência for aleatória, então qualquer subsequência extraída dela também é aleatória, devendo ser aprovada em qualquer teste de aleatoriedade.

Cada teste examina a qualidade da aleatoriedade da sequência a partir de um aspecto específico, comparando determinadas propriedades estatísticas com a estatística esperada. Assim, nesse contexto, a aleatoriedade é uma propriedade que pode ser descrita em termos de probabilidade. Um teste estatístico é formulado para testar uma hipótese nula específica, denominada H_0 , que é a de que a sequência testada é aleatória. Associada a essa hipótese nula existe a hipótese alternativa, denominada H_a , que é a de que a sequência testada não é aleatória. A partir de uma distribuição teórica de referência dos possíveis valores que a estatística do teste, que é denotada por S , pode assumir, é definido um valor crítico para essa estatística, sendo denotado por t . Assim, em cada teste, se $S > t$, então H_0 é rejeitada (H_a é aceita), enquanto que se $S \leq t$, então H_0 é aceita. A Tabela 5.1 mostra as conclusões possíveis quando um teste estatístico é realizado.

Tabela 5.1: Conclusões de um teste estatístico.

Situação Verdadeira	Conclusão	
	Aceitar H_0	Aceitar H_a (rejeitar H_0)
A sequência é aleatória (H_0 é verdadeira)	OK	Erro tipo I
A sequência não é aleatória (H_a é verdadeira)	Erro tipo II	OK

Se a sequência testada for de fato aleatória e a conclusão do teste for aceitar H_a (concluir que a sequência não é aleatória), então essa conclusão é chamada de erro tipo I. A probabilidade de ocorrência desse erro é chamada de nível de significância do teste, é denotada por α e pode ser definida *a priori*. Por outro lado, se a sequência testada de fato não for aleatória e a conclusão do teste for aceitar H_0 (concluir que a sequência é aleatória), então essa conclusão é chamada de erro tipo II. A probabilidade de ocorrência desse erro é denotada por β . Um dos principais objetivos na concepção de um teste estatístico é minimizar β , ou seja, minimizar a probabilidade de o teste aceitar uma sequência como aleatória quando de fato ela não é. Em termos da estatística e do valor crítico, tem-se $\alpha = P(S > t | H_0 \text{ é verdade}) = P(\text{rejeitar } H_0 | H_0 \text{ é verdade})$ e $\beta = P(S \leq t | H_0 \text{ é falso}) = P(\text{aceitar } H_0 | H_0 \text{ é falso})$. O valor de β , ao contrário de α não é um valor fixado. Como existem muitos aspectos de não-aleatoriedade que uma sequência binária pode ter e cada um deles leva a um valor diferente de β , então é difícil expressar o valor de β . Entretanto, os valores de α e β são relacionados entre si e com o comprimento n da sequência testada, de modo que se dois deles forem especificados, o terceiro é automaticamente determinado. Em aplicações criptográficas é comum especificar n e α . Se α for pequeno, então β é grande e vice-versa.

A estatística do teste é utilizada para calcular um valor P (denotado por *P-value*), que indica a força da evidência contra a hipótese nula, ou seja, é a probabilidade de um gerador de números aleatórios perfeito produzir uma sequência menos aleatória do que a sequência testada, considerando o aspecto de aleatoriedade avaliado pelo teste. Dado um determinado nível de significância α para o teste, se $P\text{-value} \geq \alpha$, então H_0 é aceita (a sequência aparenta ser aleatória) com uma confiança de $1 - \alpha$. Se $P\text{-value} < \alpha$, então H_0 é rejeitada (a sequência aparenta ser não-aleatória) também com uma confiança de $1 - \alpha$. Tipicamente escolhe-se α no intervalo $[0,001; 0,01]$. Em aplicações criptográficas escolhe-se tipicamente $\alpha = 0,01$, o que significa que espera-se rejeitar H_0 em menos de 1% dos casos em que as sequências são verdadeiramente aleatórias. Neste trabalho considera-se $\alpha = 0,01$.

5.2 A Suíte de Testes Estatísticos do NIST

A suíte de testes estatísticos do NIST é uma importante e popular ferramenta de análise de aleatoriedade em geradores de números pseudo-aleatórios e também de cripto-sistemas. Ela foi desenvolvida para testar as cifras que competiram para estabelecer o padrão AES [49] e tornou-se uma ferramenta frequentemente utilizada em certificações ou aprovações formais. A

versão mais atual da suíte é a 2.1.2 e consiste em 15 testes estatísticos, que foram desenvolvidos para testar a aleatoriedade de sequências binárias. A Tabela 5.2 apresenta uma descrição geral de cada um dos 15 testes.

Tabela 5.2: Descrição geral de cada um dos testes da suíte do NIST.

Teste Estatístico	Defeito Detectado
<i>Frequency (Monobit) Test</i>	Muitos zeros ou uns
<i>Frequency Test within a Block</i>	Muitos zeros ou uns
<i>Runs Test</i>	Oscilações (mudanças bruscas entre sequências de zeros ou sequências de uns) muito rápidas ou muito lentas
<i>Longest Run of Ones in a Block</i>	Desvio na distribuição de longas sequências ininterruptas de uns
<i>Binary Matrix Rank Test</i>	Desvio na distribuição do posto devido a periodicidade (subsequências que se repetem)
<i>Discrete Fourier Transform (Spectral) Test</i>	Componentes periódicos na sequência
<i>Non-overlapping Template Matching Test</i>	Muitas ocorrências de padrões não-periódicos
<i>Overlapping Template Matching Test</i>	Muitas ocorrências de blocos de uns com m bits
<i>Maurer's "Universal Statistical" Test</i>	Existência de uma subsequência que representa a sequência inteira (compressibilidade)
<i>Linear Complexity Test</i>	Desvio na distribuição do menor LFSR que gera subsequências
<i>Serial Test</i>	Distribuição não-uniforme de palavras de comprimento m
<i>Approximate Entropy Test</i>	Distribuição não-uniforme de palavras de comprimento m
<i>Cumulative Sums (Cusum) Test</i>	Muitos zeros ou uns no início da sequência
<i>Random Excursions Test</i>	Desvio na distribuição do número de visitas a um estado particular em uma caminhada aleatória
<i>Random Excursions Variant Test</i>	Desvio na distribuição do número de visitas a um estado particular através de várias caminhadas aleatórias

Alguns testes, como o *Runs Test*, o *Random Excursions Test* e o *Random Excursions Variant Test* não são sempre aplicáveis, pois eles possuem alguns pré-requisitos. O *Runs Test* é aplicável somente se a sequência for aprovada no *Frequency (Monobit) Test*. O *Random Excursions Test* e o *Random Excursions Variant Test* são aplicáveis somente se o número de ciclos de caminhada aleatória for maior ou igual a 500 [12]. Quando um teste não é aplicável seu *P-value* resultante é ajustado para zero.

Todos os testes da suíte recebem um parâmetro n , que denota o comprimento (em *bits*) da sequência processada. Assim, são testadas k sequências de n bits. Alguns testes realizam avaliações para detectar não-aleatoriedade locais e recebem um segundo parâmetro m ou M . Os testes parametrizados por m detectam o excesso de padrões de m bits (palavras) na sequência. Os testes parametrizados por M examinam a distribuição de alguma característica

específica através das $\frac{n}{M}$ partes iguais de M bits da sequência de entrada. Alguns testes da suíte do NIST examinam mais de uma propriedade da sequência de entrada, de modo que eles resultam em mais de um P -value. Um exemplo disso é o *Cumulative Sums (Cusum) Test*, que examina a sequência em sentido progressivo e regressivo, gerando dois P -values. A Tabela 5.3 apresenta os valores recomendados pelo NIST para os parâmetros recebidos por cada um dos 15 testes [12] e também a quantidade de P -values resultantes.

Tabela 5.3: Valores recomendados para os parâmetros de entrada dos testes estatísticos do NIST.

Teste	n (em bits)	m ou M (em bits)	Número de P -values
<i>Frequency (Monobit) Test</i>	$n \geq 100$	–	1
<i>Frequency Test within a Block</i>	$n \geq 100$	$M \geq 20$	1
<i>Runs Test</i>	$n \geq 100$	–	1
<i>Longest Run of Ones in a Block</i>	$n \geq 128 / n \geq 6.272 / n \geq 750.000$	$M = 8 / M = 128 / M = 10.000$	1
<i>Binary Matrix Rank Test</i>	$n \geq 38.912$	–	1
<i>Discrete Fourier Transform (Spectral) Test</i>	$n \geq 1.000$	–	1
<i>Non-overlapping Template Matching Test</i>	–	$m = 9$ ou $m = 10$	148
<i>Overlapping Template Matching Test</i>	$n \geq 10^6$	$m = 9$ ou $m = 10$	1
<i>Maurer's "Universal Statistical" Test</i>	$n \geq 387.840$ $n \geq 904.960$ $n \geq 2.068.480$ $n \geq 4.654.080$ $n \geq 10.342.400$ $n \geq 22.753.280$ $n \geq 49.643.520$ $n \geq 107.560.960$ $n \geq 231.669.760$ $n \geq 496.435.200$ $n \geq 1.059.061.760$	$L = 6$ e $Q = 640$ $L = 7$ e $Q = 1.280$ $L = 8$ e $Q = 2.560$ $L = 9$ e $Q = 5.120$ $L = 10$ e $Q = 10.240$ $L = 11$ e $Q = 20.480$ $L = 12$ e $Q = 40.960$ $L = 13$ e $Q = 81.920$ $L = 14$ e $Q = 163.840$ $L = 15$ e $Q = 327.680$ $L = 16$ e $Q = 655.360$	1
<i>Linear Complexity Test</i>	$n \geq 10^6$	$500 \leq M \leq 5.000$	1
<i>Serial Test</i>	–	$m < \lfloor \log_2 n \rfloor - 2$	2
<i>Approximate Entropy Test</i>	–	$m < \lfloor \log_2 n \rfloor - 5$	1
<i>Cumulative Sums (Cusum) Test</i>	$n \geq 100$	–	2
<i>Random Excursions Test</i>	$n \geq 10^6$	–	8
<i>Random Excursions Variant Test</i>	$n \geq 10^6$	–	18

Os parâmetros padrão da suíte de testes do NIST são apresentados na Tabela 5.4.

Tabela 5.4: Parâmetros padrão da suíte de testes do NIST.

Teste Estatístico	Parâmetros (em bits)
<i>Frequency Test within a Block</i>	$M = 128$
<i>Non-overlapping Template Matching Test</i>	$m = 9$
<i>Overlapping Template Matching Test</i>	$m = 9$
<i>Maurer's "Universal Statistical" Test</i>	$L = 7$ e $Q = 1.280$
<i>Approximate Entropy Test</i>	$m = 10$
<i>Serial Test</i>	$m = 16$
<i>Linear Complexity Test</i>	$M = 500$

Todos os testes da suíte calculam *P-values* utilizando distribuições assintóticas de referência (χ^2 ou normal) de modo que resultados razoáveis são obtidos apenas para valores apropriados de n , m e M . Considerando os parâmetros padrão da suíte do NIST, para que uma sequência gere resultados com significado estatístico em todos os 188 testes, seu comprimento deve ser maior ou igual a 1.000.000 *bits*. O NIST recomenda que, para que os resultados sejam estatisticamente relevantes, sejam testadas pelo menos $k = \alpha^{-1} = 100$ sequências [12]. Em [49], para testar as sequências binárias geradas pelos cripto-sistemas finalistas do AES, considerou-se o seguinte:

Comprimento da sequência: $n = 2^{20} = 1.048.576$ *bits*;

Número de sequências testadas: $k = 300$ sequências;

Nível de significância: $\alpha = 0,01$.

Este trabalho utiliza as mesmas premissas que foram adotadas para testar os cripto-sistemas finalistas do AES. Considera-se $k \geq 332$ nos casos em que a taxa do codificador homofônico é $\frac{1}{2}$, para garantir que $k \geq 100$ nos casos em que a taxa é maior.

Em [18], é apresentada uma versão otimizada da suíte de testes estatísticos do NIST, que diminui em aproximadamente 50,6 vezes o tempo necessário para finalizar todos os testes em uma sequência arbitrária, quando comparado com a versão 2.1.2. Na suíte do NIST, o teste que possui maior carga computacional é o *Linear Complexity Test*, que utiliza o algoritmo de Berlekamp-Massey para calcular a complexidade linear da sequência. É apresentada uma nova versão do algoritmo de Berlekamp-Massey, que calcula a complexidade linear de uma sequência sem precisar realizar a síntese do registrador linear realimentado de deslocamento. Assim, utilizando essa nova versão do algoritmo, o *Linear Complexity Test* é aproximadamente 187 mais rápido do que a versão anterior. Neste trabalho, todos os ensaios foram realizados utilizando a versão otimizada da suíte de testes estatísticos do NIST.

5.2.1 Interpretação dos Resultados

Considere k sequências sendo testadas nos 15 testes estatísticos do NIST. Considerando-se os parâmetros padrão da suíte, então, para cada sequência, são gerados 188 *P-values* (188 testes e subtestes). Seja $T_i = (P_{i1}, P_{i2}, \dots, P_{ik})$, em que $1 \leq i \leq 188$ um vetor com os *P-values* resultantes de um determinado teste, associado a cada um dos 188 testes da suíte do NIST. Então, os resultados relativos a um determinado arquivo de entrada pode ser visto como um conjunto de 188 vetores com k elementos cada.

A interpretação desses resultados gerados pelos testes estatísticos da suíte pode ser realizada de diversas maneiras. Para cada teste, o NIST realiza duas avaliações:

Teste de Proporção: avaliação da proporção de seqüências que são aprovadas no teste estatístico;

Teste de Uniformidade: avaliação da uniformidade dos *P-values* gerados pelo teste, baseada em uma distribuição de referência.

Para cada teste estatístico da suíte, se as seqüências forem reprovadas no teste de proporção ou no teste de uniformidade, elas são consideradas reprovadas no respectivo teste estatístico. Assim, para que k seqüências sejam consideradas aprovadas em um determinado teste estatístico, é necessário que elas sejam aprovadas no teste de proporção e também no teste de uniformidade.

Teste de Proporção

Dados os resultados de um teste particular, o NIST calcula a proporção de seqüências que são aprovadas nesse teste. Seja S_i o número de seqüências que obtiveram aprovação no teste T_i , em que $1 \leq i \leq 188$ (seqüência em que $P_{ij} \geq \alpha$, $1 \leq i \leq 188$, $1 \leq j \leq k$). A proporção de seqüências aprovadas no teste T_i é $Pr_i = \frac{S_i}{k}$, $1 \leq i \leq 188$. Para estabelecer um indício de não-aleatoriedade nas k seqüências testadas, define-se um *limite de confiança*, baseado na distribuição binomial. Se a proporção calculada para o teste T_i estiver abaixo desse limite, então as seqüências são reprovadas no teste de proporção.

A probabilidade de uma seqüência ser aprovada em um determinado teste é $1 - \alpha$. A probabilidade $P(S_i)$ de que das k seqüências, S_i sejam aprovadas é dada por

$$P(S_i) = \binom{k}{S_i} (1 - \alpha)^{S_i} \alpha^{k-S_i}. \quad (5.1)$$

Suponha que dentre as k seqüências submetidas ao teste T_i , F_i sejam reprovadas nesse teste. A probabilidade de que F_i seqüências falhem no teste é dada por

$$\pi_{F_i} = \binom{k}{k - F_i} (1 - \alpha)^{k-F_i} \alpha^{F_i} \quad (5.2)$$

A probabilidade de se observar F_i ou menos falhas é dada por

$$P(\text{Falhas} \leq F_i) = 1 - \sum_{j=0}^{F_i-1} \pi_j \quad (5.3)$$

Considerando que as k seqüências são reprovadas em T_i quando $P(\text{Falhas} \leq F_i) < 0,0001$, define-se o limite de confiança como a proporção associada ao número máximo de falhas tal que $P(\text{Falhas} \leq F_i) \geq 0,0001$.

Como exemplo, considere que 100 seqüências sejam submetidas a um teste T_i , em que o nível de significância seja 0,01. A Tabela 5.5 ilustra o número de falhas, a respectiva proporção associada, a probabilidade de se observar essa proporção e a probabilidade de se observar o número maior ou igual de falhas. O limite de confiança nesse caso é 0,9400, que é a proporção associada ao número máximo de falhas (6 falhas) tal que $P(\text{Falhas} \leq F_i) \geq 0,0001$.

Tabela 5.5: Limite de confiança para $k = 100$ seqüências testadas.

F_i	Proporção	π_{F_i}	$P(\text{Falhas} \leq F_i)$
0	1,0000	$\binom{100}{100}(0,99)^{100} = 0,36603$	1
1	0,9900	$\binom{100}{99}(0,99)^{99}(0,01)^1 = 0,36973$	0,63397
2	0,9800	$\binom{100}{98}(0,99)^{98}(0,01)^2 = 0,18486$	0,26423
3	0,9700	$\binom{100}{97}(0,99)^{97}(0,01)^3 = 0,06100$	0,07937
4	0,9600	$\binom{100}{96}(0,99)^{96}(0,01)^4 = 0,01494$	0,01837
5	0,9500	$\binom{100}{95}(0,99)^{95}(0,01)^5 = 0,00290$	0,00343
6	0,9400	$\binom{100}{94}(0,99)^{94}(0,01)^6 = 0,00046$	0,00053
7	0,9300	$\binom{100}{93}(0,99)^{93}(0,01)^7 = 0,00006$	0,00007

Teste de Uniformidade

Dados os resultados de um teste particular, o NIST examina a distribuição de P -values para verificar a sua uniformidade no intervalo $[0,1)$. A suíte aplica um teste χ^2 (com nove graus de liberdade) para verificar se a distribuição de P -values segue a distribuição esperada. O intervalo $[0,1)$ é dividido em 10 subintervalos $\left[\frac{i}{10}, \frac{(i+1)}{10}\right)$, $0 \leq i < 10$ e o teste χ^2 verifica se o número de P -values para cada subintervalo é próximo de $\frac{k}{10}$, onde k é o número de seqüências testadas. O teste χ^2 resulta então em um P -value $_T$ que sumariza a uniformidade dos P -values. Se esse P -value $_T$ for menor do que um nível de significância $\alpha = 0,0001$, então os P -values produzidos pelo teste são considerados não uniformes. O teste χ^2 funciona bem apenas quando $\frac{k}{10} \geq 5,5$, ou seja, o NIST recomenda que o número de seqüências testadas seja pelo menos 55.

Segundo [18], o teste χ^2 não é capaz de detectar uma possível não-uniformidade dos P -values dentro dos subintervalos. Assim, é sugerida a aplicação do teste estatístico de Kolmogorov-Smirnov (KS), que também é utilizado nas suítes TestU01 e Dieharder, para

que tais defeitos na uniformidade dos P -values sejam detectados. Neste trabalho, considera-se a utilização do teste KS utilizando os mesmos critérios de aceitação que o NIST adota para o teste χ^2 : se o P -value $_T$ resultante do teste de uniformidade for menor que 0,0001, então as sequências são consideradas não uniformes.

Os Arquivos de Saída

Cada teste da suíte, quando aplicado a sequências arbitrárias, resulta em um ou mais P -values, que são armazenados em arquivos de saída chamados “result.txt”. A suíte do NIST processa então todos os P -values de todos os arquivos “result.txt” e elabora um arquivo chamado “finalAnalysisReport.txt”, que sumariza todos os resultados de todos os testes escolhidos. A Tabela 5.6 ilustra um exemplo das informações contidas nesse arquivo, quando são processadas 1.000 sequências binárias com a suíte do NIST, cada uma possuindo 1.000.000 bits. Cada coluna da Tabela 5.6 corresponde a um teste (ou um subteste). Os valores nas colunas $C1, C2, \dots, C10$ representam o número de P -values que pertencem aos intervalos $[0, 0; 0, 1), [0, 1; 0, 2), \dots, [0, 9; 1, 0)$. No exemplo, 108 P -values calculados no *Frequency Test* pertencem ao intervalo $[0, 1; 0, 2)$. Os valores na coluna P -value representam os resultados dos testes de uniformidade para os P -values calculados nos testes estatísticos. Os valores na coluna *Proportion* representam a proporção de sequências que foram aprovadas em cada teste. Por exemplo, a proporção de sequências que foram aprovadas no *Frequency Test* é 0,991, ou seja, 991 das 1.000 sequências foram aprovadas nesse teste. Os resultados que o NIST interpreta como indício de não-aleatoriedade (falha no teste de proporção ou falha no teste de uniformidade dos P -values) são marcados com um asterisco.

Tabela 5.6: Informações parciais contidas no arquivo “finalAnalysisReport”.

$C1$	$C2$	$C3$	$C4$	$C5$	$C6$	$C7$	$C8$	$C9$	$C10$	P -value	<i>Proportion</i>	<i>Statistical Test</i>
99	108	91	105	109	104	92	101	93	98	0.920383	0.9910	<i>Frequency</i>
90	89	103	101	111	105	100	94	108	99	0.853049	0.9970	<i>BlockFrequency</i>
90	114	93	114	96	90	102	96	101	104	0.643366	0.9910	<i>CumulativeSums</i>
103	91	101	99	113	97	87	88	114	107	0.506194	0.9930	<i>CumulativeSums</i>
41	44	44	45	50	568	51	48	51	58	0.000000*	0.9970	<i>NonOverlappingTemplate</i>
41	44	49	46	47	589	54	41	51	38	0.000000*	1.0000*	<i>NonOverlappingTemplate</i>
99	107	99	113	94	100	110	87	91	100	0.733899	0.9940	<i>Serial</i>
104	116	103	96	94	95	101	102	84	105	0.695200	0.9890	<i>Serial</i>
97	107	101	111	115	90	100	94	98	87	0.622546	0.9900	<i>LinearComplexity</i>

Interpretação de Múltiplos Testes

Considere uma sequência que esteja sendo testada pelos 188 testes da suíte do NIST, considerando os parâmetros padrão. A probabilidade dessa sequência ser reprovada em i testes é $Pr(i, 188) = \binom{188}{i} (0,99)^{188-i} (0,01)^i$. A Tabela 5.7 mostra as probabilidades em percentual de uma sequência ser reprovada em i testes estatísticos. Também são mostradas as probabilidades cumulativas de a sequência ser reprovada em i ou mais testes. Considerando um nível de significância $\alpha = 0,01 = 1\%$, nota-se uma sequência pode ser considerada aleatória se ela for reprovada em até 6 testes estatísticos. Neste trabalho esse critério será estendido para o conjunto de k sequências, ou seja, se as k sequências forem reprovadas em até 6 testes estatísticos, então elas serão consideradas aleatórias. Em caso contrário, elas serão consideradas não-aleatórias.

Tabela 5.7: Probabilidades em percentual de uma sequência falhar em i testes estatísticos.

i	0	1	2	3	4	5	6	7
$Pr(i, 188)$	15,12%	28,70%	27,11%	16,98%	7,93%	2,95%	0,91%	0,24%
Cumulativo	100%	84,88%	56,18%	29,07%	12,09%	4,16%	1,21%	0,31%

Definição 5.1 (Índice NIST) Seja n_a o número de testes nos quais a sequência foi aprovada na suíte do NIST. O índice NIST é definido como $I_N = \frac{n_a}{188}$. Logo, $0 \leq I_N \leq 1$.

Obter $I_N = 1$ significa que uma sequência foi aprovada em todos os 188 testes estatísticos do NIST, enquanto que obter $I_N = 0$ significa que a sequência foi reprovada em todos os testes. Para a aplicação de codificação homofônica, considera-se que as sequências de saída do codificador são satisfatórias se $I_N \geq \frac{182}{188} \simeq 0,9681$ (limite de tolerância).

Em [50], mostra-se que até sequências produzidas por um gerador quântico de números aleatórios (fonte física) podem falhar em um ou mais testes estatísticos. Assim, nos casos onde as sequências forem consideradas não-aleatórias, recomenda-se examinar amostras adicionais para avaliar se as reprovações indicam uma anomalia estatística ou uma evidência clara de não-aleatoriedade.

CAPÍTULO 6

ANÁLISE DOS ENSAIOS ESTATÍSTICOS

6.1 Análise do Gerador de Números Pseudo-Aleatórios

Para avaliar se o gerador de números aleatórios de Park-Miller-Carta é adequado para aplicação em codificação homofônica universal, testou-se sua saída utilizando a suíte de testes estatísticos do NIST, considerando cinco sementes diferentes. Foram gerados cinco arquivos, cada um com 500 sequências de 2^{20} bits, associadas às sementes $S = 12345$, $S = 54321$, $S = 112358$, $S = 19872008$ e $S = 26011982$, escolhidas ao acaso.

Para facilitar a interpretação dos resultados dos testes, é realizada uma abordagem gráfica, em que o eixo das abscissas representa os testes individuais e o eixo das ordenadas representa a proporção de sequências aprovadas no teste estatístico correspondente, considerando o nível de significância $\alpha = 0,01$. É representado no gráfico também o *limite de confiança*. Como o gerador de números pseudo-aleatórios é um componente fundamental nos esquemas de codificação homofônica universal analisados neste trabalho, optou-se por considerar um limite de confiança mais rigoroso do que o limite definido na Seção 5.2. Assim, o limite considerado é 97,4% (até 13 sequências rejeitadas em 500). Se houver algum ponto abaixo do limite, então significa que a sequência foi reprovada no teste correspondente. As Figuras 6.1, 6.2, 6.3, 6.4 e 6.5 ilustram os resultados dos testes estatísticos para as sequências geradas pelo gerador de Park-Miller-Carta, considerando as sementes $x_{01} = 12345$, $x_{02} = 54321$, $x_{03} = 112358$, $x_{04} = 19872008$ e $x_{05} = 26011982$, respectivamente. Observa-se que, para todas as cinco sementes consideradas, a sequência de saída do gerador de Park-Miller-Carta é aprovada em

todos os testes realizados, possuindo assim propriedades estatísticas satisfatórias para utilização na aplicação de codificação homofônica universal.

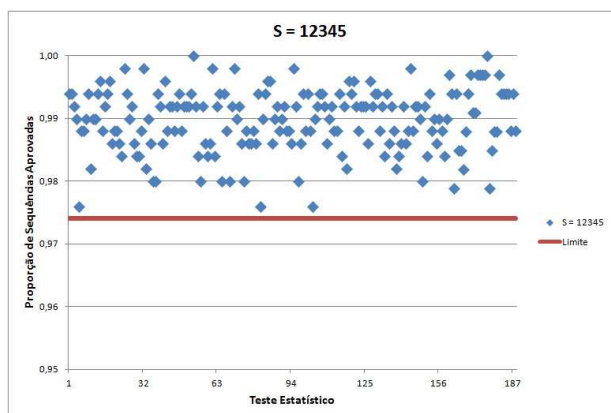


Figura 6.1: Resultados dos testes estatísticos para a semente $x_{01} = 12345$.

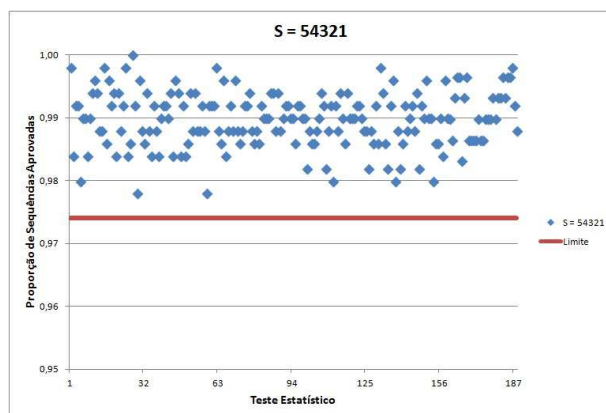


Figura 6.2: Resultados dos testes estatísticos para a semente $x_{02} = 54321$.

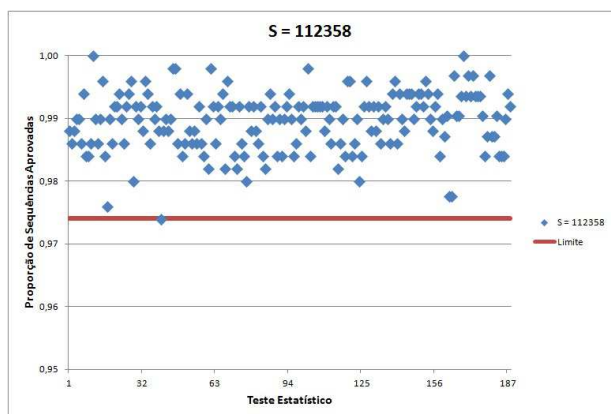


Figura 6.3: Resultados dos testes estatísticos para a semente $x_{03} = 112358$.

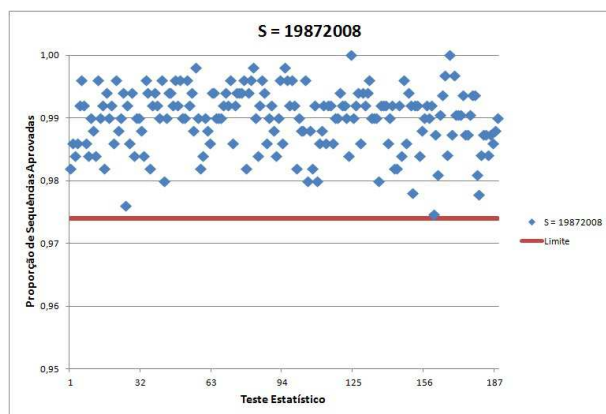


Figura 6.4: Resultados dos testes estatísticos para a semente $x_{04} = 19872008$.

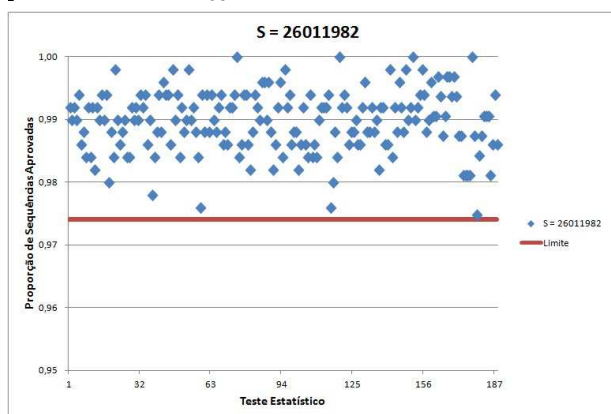


Figura 6.5: Resultados dos testes estatísticos para a semente $x_{05} = 26011982$.

6.2 Análise do Codificador OMI/DEI com $n = 1$ (Ensaio 1)

Para iniciar a análise dos codificadores OMI e DEI, considere inicialmente o caso com a pior taxa possível, ou seja, quando $n = 1$ ($R = \frac{1}{2}$). Nesse caso, os dois codificadores são equivalentes, sendo ilustrados na Figura 6.6. Nesse esquema, as chaves S_1 e S_2 operam de forma síncrona, mudando suas posições de forma sucessiva a cada ciclo.

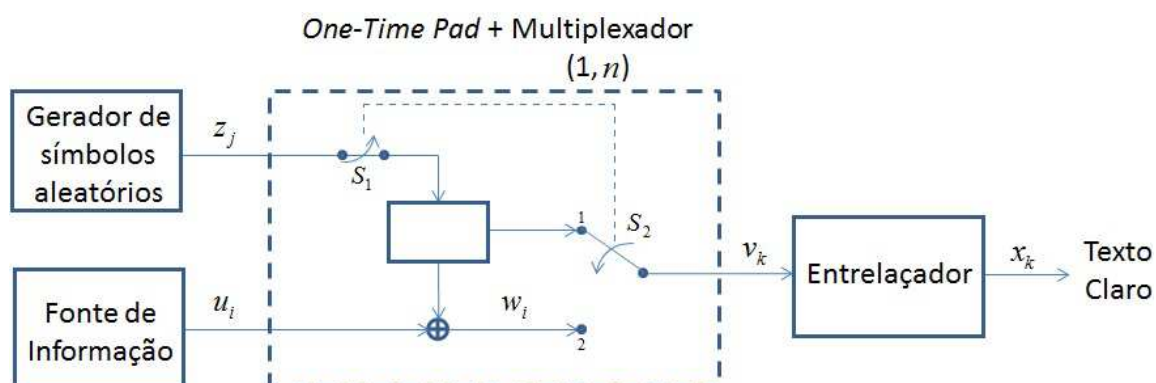


Figura 6.6: Codificador OMI/DEI com $n = 1$.

6.2.1 Fontes de Informação

Considere cinco fontes de informação, cujas informações estão na Tabela 6.1:

Tabela 6.1: Fontes consideradas para a realização dos ensaios estatísticos.

Fonte	Tipo da Fonte	Tamanho da Fonte
Agatha	Texto	27110784 bytes
Branco	Imagem <i>bitmap</i>	27000000 bytes (3000 \times 3000 <i>pixels</i>)
Cana51	Imagem <i>bitmap</i>	21784680 bytes (2338 \times 3105 <i>pixels</i>)
Platão	Imagem <i>bitmap</i>	22548448 bytes (2322 \times 3236 <i>pixels</i>)
SC06	Imagem <i>bitmap</i>	23476544 bytes (2409 \times 3248 <i>pixels</i>)

A fonte referida como “Agatha” é uma compilação de *e-books* de Agatha Christie, enquanto a fonte referida como “Branco” é uma imagem toda branca, com todos os *pixels* iguais. As Figuras 6.7, 6.8 e 6.9 ilustram as fontes referidas como “Cana51”, “Platão” e “SC06”.

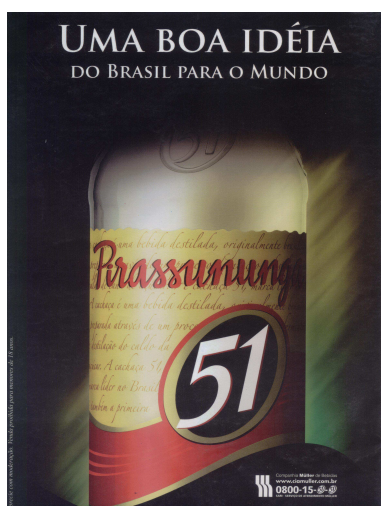


Figura 6.7: Imagem da fonte “Cana 51”.

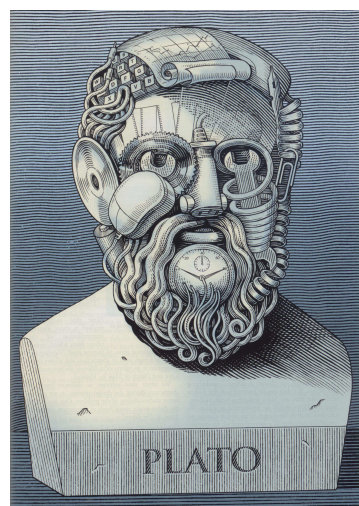


Figura 6.8: Imagem da fonte “Platão”.

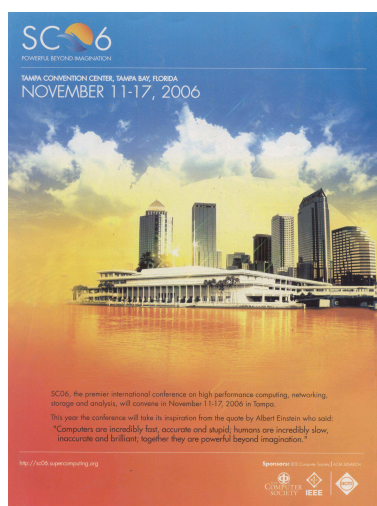


Figura 6.9: Imagem da fonte “SC06”.

As imagens adotadas neste trabalho não pertencem a nenhum repositório acadêmico de imagens, como o repositório USC-SIPI [51], por exemplo. Nos repositórios pesquisados, as fontes de informação possuem um tamanho pequeno (no caso do USC-SIPI, as maiores possuem 1024×1024 pixels), não sendo adequadas para gerar resultados estatísticos consistentes quando submetidas a uma suíte de testes, após serem processadas por um codificador homofônico universal. Um outro detalhe indesejado em relação a essas imagens é que elas são disponibilizadas em um formato diferente do *bitmap*, sendo previamente processadas por um codificador de fonte, não possuindo assim muita redundância. Quanto menos redundância tiver a fonte de informação, menor é a necessidade de processá-la com um codificador homofônico.

6.2.2 Objetivo e Metodologia do Ensaio 1

Para verificar a qualidade estatística da saída do codificador homofônico, realizou-se um ensaio utilizando a suíte de testes do NIST, variando-se os entrelaçadores e também considerando períodos e parâmetros diferentes. O objetivo deste ensaio é avaliar os seguintes itens:

- Detectar se a estrutura do entrelaçador possui influência em eventuais falhas das sequências de saída do codificador homofônico em testes específicos da suíte (reprovações persistentes);
- Avaliar a influência do período, da dispersão e do espalhamento dos entrelaçadores na qualidade estatística das sequências de saída do codificador homofônico;
- Avaliar a influência dos parâmetros específicos de cada entrelaçador na qualidade estatística das sequências de saída do codificador homofônico.

Foram considerados os entrelaçadores de Berrou-Glavieux (BGL), Co-Primo (CPR), JPL, LRTB, Takeshita-Costello (TKC) e Welch-Costas (WLC) (os resultados relativos aos entrelaçadores LRBT, RLBT e RLTB não são apresentados, pois apresentam resultados muito semelhantes ao do entrelaçador LRTB). Como o período do entrelaçador de Welch-Costas é $T = p - 1$, em que p é um número primo, são considerados períodos o mais próximos possíveis dos demais entrelaçadores para não descaracterizar as comparações entre os desempenhos estatísticos dos entrelaçadores no sistema. Os períodos e os respectivos parâmetros considerados para os entrelaçadores BGL, JPL e LRTB são apresentados na Tabela 6.2, para os entrelaçadores CPR e TKC são apresentados nas Tabelas 6.3 e 6.4 e para o entrelaçador WLC são apresentados na Tabela 6.5. Foram realizados ensaios processando cada uma das fontes de informação. No caso da Tabela 6.2, os parâmetros marcados em amarelo são aplicáveis somente ao entrelaçador LRTB, enquanto que os parâmetros marcados em cinza são aplicáveis aos entrelaçadores JPL e LRTB.

Tabela 6.2: Períodos e parâmetros considerados para os entrelaçadores BGL, JPL e LRTB.

T = 64		T = 128		T = 256		T = 512		T = 1024		T = 2048		T = 4096		T = 8192	
N	M	N	M	N	M	N	M	N	M	N	M	N	M	N	M
1	64	1	128	1	256	1	512	1	1024	1	2048	1	4096	1	8192
2	32	2	64	2	128	2	256	2	512	2	1024	2	2048	2	4096
4	16	4	32	4	64	4	128	4	256	4	512	4	1024	4	2048
8	8	8	16	8	32	8	64	8	128	8	256	8	512	8	1024
16	4	16	8	16	16	16	32	16	64	16	128	16	256	16	512
32	2	32	4	32	8	32	16	32	32	32	64	32	128	32	256
64	1	64	2	64	4	64	8	64	16	64	32	64	64	64	128
		128	1	128	2	128	4	128	8	128	16	128	32	128	64
				256	1	256	2	256	4	256	8	256	16	256	32
						512	1	512	2	512	4	512	8	512	16
								1024	1	1024	2	1024	4	1024	8
										2048	1	2048	2	2048	4
												4096	1	4096	2
														8192	1

T = 16384		T = 32768		T = 65536		T = 131072		T = 262144		T = 524288		T = 1048576	
N	M	N	M	N	M	N	M	N	M	N	M	N	M
1	16384	1	32768	1	65536	1	131072	1	262144	1	524288	1	1048576
2	8192	2	16384	2	32768	2	65536	2	131072	2	262144	2	524288
4	4096	4	8192	4	16384	4	32768	4	65536	4	131072	4	262144
8	2048	8	4096	8	8192	8	16384	8	32768	8	65536	8	131072
16	1024	16	2048	16	4096	16	8192	16	16384	16	32768	16	65536
32	512	32	1024	32	2048	32	4096	32	8192	32	16384	32	32768
64	256	64	512	64	1024	64	2048	64	4096	64	8192	64	16384
128	128	128	256	128	512	128	1024	128	2048	128	4096	128	8192
256	64	256	128	256	256	256	512	256	1024	256	2048	256	4096
512	32	512	64	512	128	512	256	512	512	512	1024	512	2048
1024	16	1024	32	1024	64	1024	128	1024	256	1024	512	1024	1024
2048	8	2048	16	2048	32	2048	64	2048	128	2048	256	2048	512
4096	4	4096	8	4096	16	4096	32	4096	64	4096	128	4096	256
8192	2	8192	4	8192	8	8192	16	8192	32	8192	64	8192	128
16384	1	16384	2	16384	4	16384	8	16384	16	16384	32	16384	64
		32768	1	32768	2	32768	4	32768	8	32768	16	32768	32
				65536	1	65536	2	65536	4	65536	8	65536	16
						131072	1	131072	2	131072	4	131072	8
								262144	1	262144	2	262144	4
										524288	1	524288	2
												1048576	1

Tabela 6.3: Períodos e parâmetros considerados para os entrelaçadores CPR e TKC (parte 1).

$T = 64$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	3	3	3	3	3	17	17	17	17	17
b (CPR) / h (TKC)	16	32	43	48	63	16	32	43	48	63
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	37	37	37	37	37	53	53	53	53	53
b (CPR) / h (TKC)	16	32	43	48	63	16	32	43	48	63
$T = 128$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	13	13	13	13	13	31	31	31	31	31
b (CPR) / h (TKC)	25	51	76	102	127	25	51	76	102	127
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	59	59	59	59	59	79	79	79	79	79
b (CPR) / h (TKC)	25	51	76	102	127	25	51	76	102	127
$T = 256$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	19	19	19	19	19	67	67	67	67	67
b (CPR) / h (TKC)	64	114	128	191	255	64	114	128	191	255
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	131	131	131	131	131	211	211	211	211	211
b (CPR) / h (TKC)	64	114	128	191	255	64	114	128	191	255
$T = 512$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	23	23	23	23	23	103	103	103	103	103
b (CPR) / h (TKC)	102	204	307	409	511	102	204	307	409	511
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	223	223	223	223	223	307	307	307	307	307
b (CPR) / h (TKC)	102	204	307	409	511	102	204	307	409	511
$T = 1024$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	5	5	5	5	5	257	257	257	257	257
b (CPR) / h (TKC)	256	300	512	767	1023	256	300	512	767	1023
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	523	523	523	523	523	769	769	769	769	769
b (CPR) / h (TKC)	256	300	512	767	1023	256	300	512	767	1023
$T = 2048$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	7	7	7	7	7	409	409	409	409	409
b (CPR) / h (TKC)	409	819	1228	1638	2047	409	819	1228	1638	2047
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	821	821	821	821	821	1229	1229	1229	1229	1229
b (CPR) / h (TKC)	409	819	1228	1638	2047	409	819	1228	1638	2047
$T = 4096$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	11	11	11	11	11	1031	1031	1031	1031	1031
b (CPR) / h (TKC)	44	1024	2048	3071	4095	44	1024	2048	3071	4095
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	2053	2053	2053	2053	2053	3851	3851	3851	3851	3851
b (CPR) / h (TKC)	44	1024	2048	3071	4095	44	1024	2048	3071	4095
$T = 8192$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	29	29	29	29	29	1657	1657	1657	1657	1657
b (CPR) / h (TKC)	1638	3276	4915	6553	8191	1638	3276	4915	6553	8191
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	3299	3299	3299	3299	3299	4919	4919	4919	4919	4919
b (CPR) / h (TKC)	1638	3276	4915	6553	8191	1638	3276	4915	6553	8191
$T = 16384$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	41	41	41	41	41	6079	6079	6079	6079	6079
b (CPR) / h (TKC)	4096	8192	12287	15321	16383	4096	8192	12287	15321	16383
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	8209	8209	8209	8209	8209	12289	12289	12289	12289	12289
b (CPR) / h (TKC)	4096	8192	12287	15321	16383	4096	8192	12287	15321	16383
$T = 32768$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	43	43	43	43	43	6553	6553	6553	6553	6553
b (CPR) / h (TKC)	6553	13107	19660	26214	32767	6553	13107	19660	26214	32767
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	13109	13109	13109	13109	13109	19661	19661	19661	19661	19661
b (CPR) / h (TKC)	6553	13107	19660	26214	32767	6553	13107	19660	26214	32767
$T = 65536$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	761	761	761	761	761	16411	16411	16411	16411	16411
b (CPR) / h (TKC)	87	16384	32768	49151	65535	87	16384	32768	49151	65535
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	32771	32771	32771	32771	32771	65521	65521	65521	65521	65521
b (CPR) / h (TKC)	87	16384	32768	49151	65535	87	16384	32768	49151	65535
$T = 131072$										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	61	61	61	61	61	26227	26227	26227	26227	26227
b (CPR) / h (TKC)	26214	52428	78643	104857	131071	26214	52428	78643	104857	131071
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	52433	52433	52433	52433	52433	78643	78643	78643	78643	78643
b (CPR) / h (TKC)	26214	52428	78643	104857	131071	26214	52428	78643	104857	131071

Tabela 6.4: Períodos e parâmetros considerados para os entrelaçadores CPR e TKC (parte 2).

T = 262144										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	71	71	71	71	71	53231	53231	53231	53231	53231
b (CPR) / h (TKC)	53215	65536	131072	196607	262143	53215	65536	131072	196607	262143
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	104729	104729	104729	104729	104729	131101	131101	131101	131101	131101
b (CPR) / h (TKC)	53215	65536	131072	196607	262143	53215	65536	131072	196607	262143
T = 524288										
Caso	1	2	3	4	5	6	7	8	9	10
a (CPR) / k (TKC)	76393	76393	76393	76393	76393	292321	292321	292321	292321	292321
b (CPR) / h (TKC)	37017	144933	270957	338852	436241	37017	144933	270957	338852	436241
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	351119	351119	351119	351119	351119	397057	397057	397057	397057	397057
b (CPR) / h (TKC)	37017	144933	270957	338852	436241	37017	144933	270957	338852	436241
T = 1048576										
a (CPR) / k (TKC)	192317	192317	192317	192317	192317	481933	481933	481933	481933	481933
b (CPR) / h (TKC)	3041	233033	613437	678997	1040637	3041	233033	613437	678997	1040637
Caso	11	12	13	14	15	16	17	18	19	20
a (CPR) / k (TKC)	572819	572819	572819	572819	572819	1004871	1004871	1004871	1004871	1004871
b (CPR) / h (TKC)	3041	233033	613437	678997	1040637	3041	233033	613437	678997	1040637

Tabela 6.5: Períodos e parâmetros considerados para o entrelaçador WLC.

$T = 60$										
$p = 61$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	7	17	18	26	31	35	43	51	55
$T = 126$										
$p = 127$										
Caso	1	2	3	4	5	6	7	8	9	10
α	3	14	29	39	53	65	78	91	106	116
$T = 256$										
$p = 257$										
Caso	1	2	3	4	5	6	7	8	9	10
α	3	27	53	78	103	130	155	180	206	233
$T = 508$										
$p = 509$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	51	108	155	204	255	306	358	411	459
$T = 1020$										
$p = 1021$										
Caso	1	2	3	4	5	6	7	8	9	10
α	10	103	209	309	410	516	619	715	823	919
$T = 2052$										
$p = 2053$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	209	412	620	827	1027	1232	1443	1643	1851
$T = 4092$										
$p = 4093$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	410	822	1232	1639	2047	2456	2867	3275	3686
$T = 8190$										
$p = 8191$										
Caso	1	2	3	4	5	6	7	8	9	10
α	17	823	1641	2458	3282	4104	4916	5737	6564	7378
$T = 16380$										
$p = 16381$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	1639	3280	4919	6559	8191	9829	11472	13106	14753
$T = 32770$										
$p = 32771$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	3279	6559	9835	13110	16386	19663	22942	26218	29495
$T = 65536$										
$p = 65537$										
Caso	1	2	3	4	5	6	7	8	9	10
α	3	6555	13109	19662	26215	32770	39323	45876	52430	58985
$T = 131070$										
$p = 131071$										
Caso	1	2	3	4	5	6	7	8	9	10
α	3	13109	26218	39325	52429	65537	78645	91750	104858	117966
$T = 262146$										
$p = 262147$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	26215	52440	78646	104859	131074	157289	183507	209729	235935
$T = 524286$										
$p = 524287$										
Caso	1	2	3	4	5	6	7	8	9	10
α	3	52308	104907	157265	209605	261706	314142	366647	418783	470725
$T = 1048572$										
$p = 1048573$										
Caso	1	2	3	4	5	6	7	8	9	10
α	2	104355	209535	314375	419662	524290	628920	734220	839057	944236

Foram realizados 9750 ensaios estatísticos, considerando as cinco fontes de informação listadas na Tabela 6.1 e a semente $x_0 = 12345$ no gerador de Park-Miller-Carta. Neste capítulo, são apresentados somente os resultados relativos à fonte “Branco”, pois ela representa o pior caso para o problema de codificação homofônica, pois possui entropia nula porque a imagem tem todos os *pixels* iguais. Considera-se neste trabalho a premissa de que se for realizada uma codificação homofônica eficiente em uma fonte com entropia nula, então ela também será eficiente para qualquer outra fonte de informação. Os resultados desse ensaio, considerando as demais fontes de informação, são apresentados no Apêndice B.

Para cada entrelaçador, os resultados dos ensaios são apresentados sob a forma de uma figura de uma tabela, em que cada célula representa o valor do índice NIST I_N para uma determinada combinação de parâmetros. Se o índice NIST de um determinado ensaio for menor do que o limite de tolerância $\left(I_N \geq \frac{182}{188} \simeq 0,9681\right)$, então a célula correspondente é marcada em vermelho, indicando uma reprovação, enquanto que se I_N for maior ou igual ao limite de tolerância, então a célula é marcada em verde, indicando uma aprovação.

6.2.3 Resultados Envolvendo o Entrelaçador BGL

A Figura 6.10 apresenta os resultados do Ensaio 1, envolvendo o entrelaçador BGL, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I _N - Branco - BGL																			
T	N																		
	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576	
64	0,33%	2,96%	0,33%	77,13%															
128	47,34%	1,60%	4,79%	0,00%	77,13%														
256	48,94%	81,38%	1,06%	4,79%	0,00%	77,66%													
512	81,91%	80,32%	81,91%	1,06%	4,79%	0,00%	77,66%												
1024	81,91%	81,38%	82,98%	81,38%	0,53%	5,32%	0,00%	76,60%											
2048	83,51%	82,98%	82,45%	83,51%	81,38%	1,60%	5,32%	0,00%	78,72%										
4096	84,04%	82,98%	84,04%	83,51%	82,45%	81,38%	1,06%	4,79%	0,00%	77,13%									
8192	82,98%	81,91%	84,57%	83,51%	82,45%	82,98%	81,38%	1,06%	4,79%	0,00%	77,66%								
16384	85,64%	86,70%	87,23%	89,36%	85,64%	87,23%	85,11%	81,38%	1,60%	4,79%	0,00%	82,45%							
32768	89,89%	90,96%	90,96%	91,49%	91,49%	91,49%	86,79%	83,11%	81,38%	1,06%	4,79%	0,53%	84,04%						
65536	97,87%	97,02%	94,15%	95,21%	93,21%	94,15%	97,34%	96,43%	83,51%	81,38%	1,06%	5,32%	1,06%	88,30%					
131072	97,87%	97,87%	97,87%	96,81%	96,81%	97,34%	96,28%	96,81%	88,83%	83,51%	81,38%	1,60%	5,32%	1,06%	91,09%				
262144	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,81%	96,28%	84,57%	81,91%	80,85%	1,06%	4,79%	2,13%	96,28%			
524288	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	90,43%	82,98%	83,51%	81,91%	1,60%	6,91%	1,06%	95,21%		
1048576	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,28%	89,89%	83,51%	82,98%	81,91%	2,13%	4,79%	0,00%	95,21%	

Figura 6.10: Resultados do Ensaio 1 envolvendo o entrelaçador BGL.

Em todos os testes realizados, não foram detectadas reprovações persistentes em nenhum teste estatístico específico. Assim, considera-se que o entrelaçador BGL não apresenta uma estrutura que seja responsável pelo aparecimento de padrões na sequência de saída do codificador homofônico, sendo considerado adequado para a aplicação.

Quando se utiliza o entrelaçador BGL, I_N atinge valores maiores com o aumento do período do entrelaçador. Supondo $T = 2^k$, considera-se uma codificação homofônica eficiente para

essa fonte quando $k \geq 17$. Para cada período nesse intervalo, os resultados são satisfatórios se considerarmos $N = 2^n$, em que $n \leq \left\lfloor \frac{k}{2} \right\rfloor + 1$ (a única exceção ocorre quando $T = 131072$ e $N = 512$).

Para as outras fontes, encontra-se resultados satisfatórios quando $T \geq 256$ (ver Apêndice B). Assim, se for considerado um critério que contemple o pior caso, considera-se que o codificador OMI/DEI com $n = 1$ pode ser utilizado com segurança utilizando o entrelaçador BGL se $T \geq 131072$. Se for considerado um critério mais relaxado, pois não é muito provável se deparar com fontes de entropia nula em aplicações práticas, pode-se considerar $T \geq 256$, diminuindo significativamente a quantidade de memória necessária para implementar o entrelaçador.

6.2.4 Resultados Envolvendo o Entrelaçador JPL

A Figura 6.11 apresenta os resultados do Ensaio 1, envolvendo o entrelaçador JPL, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I _N - Branco - JPL		N																			
T	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576	
64	81,38%	0,53%	1,72%	4,79%	0,53%	0,00%															
128	82,45%	82,45%	0,53%	2,13%	4,79%	0,53%	0,00%														
256	82,98%	82,98%	1,60%	0,53%	2,66%	4,79%	0,53%	0,00%													
512	83,51%	82,98%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%												
1024	83,51%	81,91%	81,38%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%											
2048	84,04%	84,04%	80,85%	79,79%	1,60%	1,06%	0,53%	2,13%	4,79%	0,53%	0,00%										
4096	84,04%	84,04%	83,51%	80,32%	78,72%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%									
8192	83,51%	84,04%	83,51%	82,45%	80,85%	80,85%	1,60%	1,06%	0,53%	2,13%	4,79%	0,53%	0,00%								
16384	86,70%	84,04%	82,98%	82,98%	82,45%	79,79%	81,38%	1,60%	0,53%	2,13%	4,79%	0,53%	0,00%								
32768	80,45%	87,23%	84,04%	83,51%	82,98%	82,98%	80,32%	80,85%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%						
65536	95,74%	91,49%	86,70%	82,98%	82,98%	82,98%	79,79%	80,85%	1,60%	1,06%	0,53%	2,13%	4,79%	0,53%	0,00%						
131072	97,34%	97,34%	90,43%	86,70%	82,98%	84,04%	81,91%	82,98%	80,32%	80,85%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%				
262144	97,87%	97,87%	95,21%	90,96%	87,77%	84,04%	84,04%	82,98%	82,98%	80,85%	79,79%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%			
524288	97,87%	97,87%	97,34%	96,81%	91,49%	87,77%	84,57%	82,98%	82,45%	82,98%	81,38%	79,79%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%		
1048576	97,87%	97,87%	97,87%	97,34%	96,28%	90,96%	88,83%	84,04%	84,04%	82,98%	82,98%	80,85%	80,32%	1,60%	1,06%	0,53%	2,66%	4,79%	0,53%	0,00%	

Figura 6.11: Resultados do Ensaio 1 envolvendo o entrelaçador JPL.

Em todos os testes realizados, foi detectada uma reprovação persistente no *Discrete Fourier Transform (Spectral) Test* em quatro das cinco fontes de informação, para todos os períodos e parâmetros considerados. Isso indica uma fraqueza introduzida pelo entrelaçador: a geração de padrões repetitivos próximos entre si na sequência de saída do codificador homofônico. Essa reprovação persistente foi observada mesmo nos casos em que o índice NIST é igual ou superior ao limite de tolerância. Assim, devido a essa potencial vulnerabilidade estatística, o entrelaçador JPL é considerado inadequado para as aplicações de codificação homofônica universal analisadas neste trabalho.

6.2.5 Resultados Envolvendo o Entrelaçador LRTB

A Figura 6.12 apresenta os resultados do Ensaio 1, envolvendo o entrelaçador LRTB, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I _N - Branco - LRTB		N																					
T	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576		
64	0,00%	0,53%	0,53%	1,06%	80,32%	81,91%	0,00%																
128	0,00%	0,53%	0,53%	1,06%	80,32%	82,45%	81,91%	0,00%															
256	0,00%	0,53%	0,53%	1,06%	80,32%	81,38%	81,91%	80,32%	0,00%														
512	0,00%	0,53%	0,53%	1,06%	80,85%	80,32%	81,91%	80,85%	80,85%	0,00%													
1024	0,00%	0,53%	0,53%	1,06%	79,26%	82,45%	81,38%	80,85%	80,85%	80,85%	0,00%												
2048	0,00%	0,53%	0,53%	1,06%	80,85%	81,91%	81,91%	80,32%	80,32%	80,85%	80,85%	0,00%											
4096	0,00%	0,53%	0,53%	1,06%	80,85%	81,91%	80,32%	81,38%	80,32%	79,79%	80,85%	80,85%	0,00%										
8192	0,00%	0,53%	0,53%	1,06%	80,85%	79,26%	80,85%	80,85%	80,85%	80,32%	81,38%	80,32%	0,00%										
16384	0,00%	0,53%	0,53%	1,06%	80,85%	82,45%	81,38%	80,85%	80,85%	80,32%	80,85%	81,38%	80,85%	84,57%	0,00%								
32768	0,00%	0,53%	0,53%	1,06%	80,32%	81,91%	80,85%	80,32%	80,32%	80,85%	80,32%	80,85%	80,85%	84,04%	86,70%	0,00%							
65536	0,00%	0,53%	0,53%	1,06%	80,85%	82,45%	80,32%	80,85%	79,79%	79,79%	80,85%	80,85%	80,32%	84,57%	87,17%	82,62%	0,00%						
131072	0,00%	0,53%	0,53%	1,06%	80,85%	82,45%	80,32%	80,85%	80,85%	80,32%	81,38%	79,79%	84,04%	88,63%	92,55%	94,15%	0,00%						
262144	0,00%	0,53%	0,53%	1,06%	80,85%	82,45%	80,85%	80,32%	80,32%	80,32%	79,26%	79,26%	80,85%	83,51%	86,70%	91,62%	91,62%	94,68%	0,00%				
524288	0,00%	0,53%	0,53%	1,06%	80,32%	81,91%	80,85%	79,79%	79,79%	79,79%	80,32%	80,32%	79,26%	83,51%	88,10%	91,49%	93,62%	94,68%	94,15%	0,00%			
1048576	0,00%	0,53%	0,53%	1,06%	80,85%	81,38%	80,32%	80,85%	79,26%	80,32%	80,85%	80,85%	81,91%	84,04%	86,70%	92,55%	92,55%	95,21%	94,68%	94,68%	0,00%		

Figura 6.12: Resultados do Ensaio 1 envolvendo o entrelaçador LRTB.

Em todos os testes realizados, o índice NIST possui valor abaixo do limite de tolerância. Além disso, foi detectada uma reprovação persistente no *Discrete Fourier Transform (Spectral) Test* em todas as fontes de informação, para todos os períodos e parâmetros considerados. Como esse entrelaçador possui a mesma vulnerabilidade estatística do entrelaçador JPL e também não foram observados casos de sucesso nos períodos considerados, conclui-se que ele é considerado inadequado para as aplicações de codificação homofônica universal analisadas neste trabalho.

6.2.6 Resultados Envolvendo o Entrelaçador CPR

Para os testes envolvendo o entrelaçador CPR, considere 20 casos para cada um dos períodos, apresentados nas Tabelas 6.3 e 6.4.

A Figura 6.13 apresenta os resultados do Ensaio 1, envolvendo o entrelaçador CPR, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I _N - Branco - CPR																				
T	Caso																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
64	82,45%	82,45%	82,45%	82,45%	82,45%	80,32%	80,89%	80,32%	80,89%	79,79%	82,45%	82,45%	82,98%	82,98%	82,45%	79,79%	78,72%	78,19%	80,89%	80,32%
128	82,45%	82,45%	82,98%	82,45%	82,98%	83,51%	83,51%	83,51%	83,51%	80,85%	80,85%	80,85%	80,85%	80,85%	81,91%	83,51%	82,45%	83,51%	82,45%	82,45%
256	82,98%	82,98%	82,98%	82,98%	82,45%	83,51%	83,51%	82,98%	83,51%	82,45%	82,98%	82,98%	82,45%	83,51%	82,98%	82,98%	82,98%	82,98%	82,98%	82,98%
512	82,98%	83,51%	82,98%	82,98%	82,98%	83,51%	82,98%	84,04%	84,04%	82,98%	82,98%	83,51%	82,98%	83,51%	82,98%	0,53%	1,06%	0,53%	0,53%	0,53%
1024	83,51%	83,51%	83,51%	83,51%	82,98%	82,45%	82,98%	82,45%	82,45%	82,45%	84,04%	82,98%	82,98%	82,45%	83,51%	84,04%	83,51%	83,51%	82,98%	82,98%
2048	83,51%	83,51%	83,51%	83,51%	83,51%	84,04%	84,04%	84,04%	84,04%	84,04%	84,04%	82,98%	83,51%	84,04%	83,51%	83,51%	0,53%	0,53%	0,53%	0,53%
4096	82,98%	84,04%	84,04%	84,04%	84,04%	84,04%	84,04%	84,04%	84,04%	84,04%	83,51%	83,51%	83,51%	84,04%	84,04%	84,04%	84,04%	83,51%	83,51%	83,51%
8192	84,57%	84,04%	83,51%	84,04%	85,11%	83,51%	83,51%	84,57%	83,51%	84,04%	83,51%	84,57%	83,51%	84,04%	82,98%	82,98%	81,91%	83,51%	82,98%	83,51%
16384	87,77%	87,77%	87,23%	86,17%	86,70%	87,77%	87,77%	88,83%	88,30%	88,83%	88,83%	88,30%	87,77%	87,23%	87,23%	88,83%	88,30%	87,23%	87,77%	87,77%
32768	90,96%	90,96%	91,49%	92,02%	90,43%	90,96%	91,49%	91,49%	92,02%	93,09%	90,43%	90,43%	90,43%	90,96%	89,36%	0,53%	0,53%	0,53%	0,53%	0,53%
65536	95,21%	97,34%	97,34%	96,81%	96,28%	95,21%	96,81%	96,28%	96,81%	96,28%	96,81%	96,28%	96,81%	96,81%	93,09%	92,55%	95,74%	95,21%	94,68%	96,28%
131072	97,87%	97,87%	97,34%	97,34%	97,87%	96,81%	96,81%	96,81%	96,81%	96,81%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
262144	97,34%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%	97,87%	97,87%	97,87%	97,34%	97,34%	97,87%	97,87%	97,87%	97,87%
524288	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
1048576	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%

Figura 6.13: Resultados do Ensaio 1 envolvendo o entrelaçador CPR.

Em todos os testes realizados, foi detectada uma reprovação persistente no *Discrete Fourier Transform (Spectral) Test* em todas as fontes de informação, para todos os períodos e parâmetros considerados. Essa reprovação persistente foi observada mesmo nos casos em que o índice NIST é superior ou igual ao limite de tolerância. Assim, devido a essa potencial vulnerabilidade estatística, o entrelaçador JPL é considerado inadequado para as aplicações de codificação homofônica universal analisadas neste trabalho.

6.2.7 Resultados Envolvendo o Entrelaçador TKC

Para os testes envolvendo o entrelaçador TKC, considere 20 casos para cada um dos períodos, apresentados nas Tabelas 6.3 e 6.4.

A Figura 6.14 apresenta o resultado do Ensaio 1, envolvendo o entrelaçador TKC, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I _N - Branco - TKC																				
T	Caso																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
64	25,93%	27,66%	24,47%	26,60%	26,60%	19,68%	19,68%	19,15%	19,15%	19,68%	10,11%	10,11%	10,64%	9,57%	11,17%	8,51%	8,51%	3,19%	8,51%	8,51%
128	13,83%	13,83%	13,83%	17,55%	12,77%	23,94%	21,28%	26,06%	23,40%	23,40%	25,53%	27,66%	18,62%	18,62%	26,06%	20,74%	21,81%	20,21%	20,74%	20,21%
256	46,28%	52,66%	46,28%	46,81%	54,79%	49,47%	50,53%	48,40%	50,53%	49,47%	54,25%	52,66%	53,19%	53,72%	53,19%	52,13%	46,28%	45,21%	44,15%	48,94%
512	63,30%	63,83%	61,17%	63,30%	62,77%	62,77%	65,43%	65,43%	65,43%	63,30%	70,74%	70,21%	70,74%	75,53%	71,28%	68,09%	69,15%	67,62%	68,62%	68,09%
1024	81,38%	81,91%	81,38%	81,38%	81,91%	81,91%	81,91%	80,85%	80,85%	81,38%	81,91%	81,91%	82,45%	82,45%	82,45%	78,72%	78,72%	78,72%	78,72%	78,72%
2048	81,91%	82,98%	82,98%	82,98%	82,98%	82,45%	82,45%	82,98%	82,98%	82,98%	83,51%	84,04%	83,51%	83,51%	83,51%	83,51%	83,51%	83,51%	83,51%	83,51%
4096	82,98%	82,98%	82,98%	82,98%	81,91%	81,91%	81,91%	81,91%	81,91%	81,91%	80,85%	80,85%	80,85%	80,85%	80,85%	84,04%	84,04%	82,98%	84,04%	82,98%
8192	84,04%	84,57%	83,51%	84,04%	84,04%	82,98%	82,98%	82,98%	82,45%	82,98%	83,51%	82,98%	82,98%	82,98%	82,98%	82,98%	82,98%	82,98%	82,98%	82,98%
16384	86,70%	86,17%	85,11%	86,17%	86,70%	87,77%	87,23%	87,23%	86,70%	87,23%	87,77%	87,23%	86,70%	86,70%	87,23%	85,11%	87,23%	87,23%	87,23%	87,23%
32768	90,96%	89,89%	91,49%	92,55%	91,49%	89,89%	90,96%	91,49%	90,43%	90,43%	90,43%	90,43%	90,43%	89,36%	89,89%	90,96%	92,02%	92,02%	91,49%	90,43%
65536	97,34%	97,34%	96,81%	96,81%	98,40%	96,81%	95,74%	97,34%	98,40%	97,87%	97,34%	98,40%	97,34%	98,40%	96,81%	95,21%	94,15%	97,34%	97,34%	96,28%
131072	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
262144	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
524288	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
1048576	97,87%	97,87%	97,87%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%

Figura 6.14: Resultados do Ensaio 1 envolvendo o entrelaçador TKC.

Em todos os testes realizados, não foram detectadas reprovações persistentes em nenhum teste estatístico específico. Assim, considera-se que o entrelaçador TKC não apresenta uma estrutura que seja responsável pelo aparecimento de padrões na sequência de saída do codificador homofônico, sendo considerado adequado para a aplicação.

Quando se utiliza o entrelaçador TKC, I_N atinge valores maiores com o aumento do período do entrelaçador. Supondo $T = 2^k$, considera-se uma codificação homofônica eficiente para essa fonte quando $k \geq 16$ (em 16 dos 20 casos houve sucesso quando $k = 16$).

Para as outras fontes, encontra-se resultados satisfatórios quando $T \geq 2048$ (ver Apêndice B). Assim, se for considerado um critério que contemple o pior caso, considera-se que o codificador OMI/DEI com $n = 1$ pode ser utilizado com segurança utilizando o entrelaçador TKC se $T \geq 131072$. Se for considerado um critério mais relaxado, pois não é muito provável se deparar com fontes de entropia nula em aplicações práticas, pode-se considerar $T \geq 2048$, diminuindo significativamente a quantidade de memória necessária para implementar o entrelaçador (ver o Apêndice B).

6.2.8 Resultados Envolvendo o Entrelaçador WLC

Para os testes envolvendo o entrelaçador WLC, considere 10 casos para cada um dos períodos, apresentados na Tabela 6.5.

A Figura 6.15 apresenta o resultado do Ensaio 1, envolvendo o entrelaçador WLC, processando a fonte “Branco” com o codificador OMI/DEI com $n = 1$.

I_N - Branco - WLC										
T	Caso									
	1	2	3	4	5	6	7	8	9	10
60	12,23%	2,66%	21,81%	21,81%	2,13%	13,30%	3,19%	27,13%	9,04%	30,85%
126	31,38%	11,17%	34,04%	32,45%	42,02%	32,45%	15,96%	41,49%	33,51%	16,49%
256	35,11%	43,09%	48,40%	54,26%	47,87%	47,34%	50,53%	55,32%	57,45%	37,23%
508	73,94%	70,74%	69,68%	72,34%	76,60%	77,13%	69,68%	68,62%	67,02%	68,62%
1020	81,38%	81,91%	80,32%	79,79%	81,91%	81,38%	81,38%	81,91%	80,32%	81,91%
2052	81,38%	80,85%	82,98%	82,98%	80,85%	82,98%	82,98%	83,51%	83,51%	83,51%
4092	83,51%	81,91%	82,98%	82,98%	82,45%	83,51%	82,98%	83,51%	80,85%	82,98%
8190	83,51%	81,91%	84,04%	84,04%	82,98%	81,38%	82,98%	84,04%	84,04%	83,51%
16380	84,04%	84,04%	81,91%	83,51%	82,98%	81,91%	82,98%	84,04%	84,57%	82,98%
32770	90,43%	90,43%	87,77%	89,36%	89,89%	88,83%	87,77%	90,43%	90,43%	90,43%
65536	93,09%	96,28%	97,34%	94,68%	96,28%	97,34%	97,34%	96,28%	94,15%	95,21%
131070	97,34%	97,87%	98,40%	97,87%	98,40%	98,40%	97,34%	97,34%	98,40%	98,40%
262146	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
524286	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
1048572	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%

Figura 6.15: Resultados do Ensaio 1 envolvendo o entrelaçador WLC.

Em todos os testes realizados, não foram detectadas reprovações persistentes em nenhum teste estatístico específico. Assim, considera-se que o entrelaçador WLC não apresenta uma estrutura que seja responsável pelo aparecimento de padrões na saída do codificador homofônico, sendo considerado adequado para a aplicação.

Quando se utiliza o entrelaçador WLC, I_N atinge valores maiores com o aumento do período do entrelaçador. Considera-se uma codificação homofônica eficiente para essa fonte quando $T \geq 131070$.

Para as outras fontes, encontra-se resultados satisfatórios quando $T \geq 508$ (ver Apêndice B). Assim, se for considerado um critério que contemple o pior caso, considera-se que o codificador OMI/DEI com $n = 1$ pode ser utilizado com segurança utilizando o entrelaçador TKC se $T \geq 131070$. Se for considerado um critério mais relaxado, pois não é muito provável se deparar com fontes de entropia nula em aplicações práticas, pode-se considerar $T \geq 508$, diminuindo significativamente a quantidade de memória necessária para implementar o entrelaçador.

6.2.9 Comentários para o Ensaio 1

Os resultados apresentados para o Ensaio 1 dão indicações que quais dos entrelaçadores considerados não são apropriados para serem aplicados nos esquemas de codificação homofônica universal OMI e DEI. Considerando $n = 1$, os entrelaçadores que são considerados satisfatórios para serem utilizados nos esquemas são o BGL, o TKC e o WLC. O parâmetro dos entrelaçadores que impacta mais na qualidade estatística da sequência de saída do codificador homofônico é o período T . Os parâmetros k e h do entrelaçador TKC e o parâmetro α do entrelaçador WLC não exercem influência significativa na qualidade estatística da sequência de saída do codificador homofônico, quando são variados. Nesses três casos, considera-se seguro utilizar um período da ordem de 2^{17} , levando em conta o pior caso. Se o critério for mais relaxado, levando-se em conta as outras fontes de informação, o entrelaçador que demanda menos memória para atingir bons resultados é o BGL, que necessita de apenas $T = 256$ para apresentar bons resultados nos testes estatísticos da suíte do NIST (ver Apêndice B).

Valores altos de dispersão, aliados à estrutura do entrelaçador, contribuem para uma melhor qualidade estatística na sequência de saída dos codificadores homofônicos universais. Por exemplo, considere os entrelaçadores TKC e WLC, que apresentam altas dispersões normalizadas $\gamma = 0,74$ (aproximadamente) e $\gamma = 1$, respectivamente, para todos os períodos

considerados. Nenhuma reprovação persistente é observada quando eles são utilizados, não havendo uma falha sistemática ocasionada por sua estrutura. Os entrelaçadores que são considerados inadequados para a aplicação possuem dispersão bem mais baixa do que os que são considerados adequados, como o LRTB e o CPR, para um período específico. Entretanto, isso não é uma regra, pois há casos em que um entrelaçador apropriado obtém sucesso nos testes do NIST possuindo dispersão menor do que um que não obteve. Considere, por exemplo, os entrelaçadores BGL e JPL e os períodos $T_1 = 131072$ e $T_2 = 262144$. Fazendo $N = 2^n$, a Tabela 6.6 apresenta os valores das dispersões normalizadas para esses períodos para $3 \leq n \leq 18$. As células marcadas em verde indicam casos de sucesso nos ensaios, enquanto que as células marcadas em vermelho indicam os casos de falha.

Tabela 6.6: Dispersões normalizadas dos entrelaçadores BGL e JPL para $T_1 = 131072$ e $T_2 = 262144$.

$T_1 = 131072$			$T_2 = 262144$		
N	γ_{BGL}	γ_{JPL}	N	γ_{BGL}	γ_{JPL}
8	0,353318	0,154161	8	0,353292	0,298866
16	0,224177	0,099021	16	0,224127	0,268228
32	0,130969	0,054627	32	0,130912	0,153962
64	0,071271	0,028939	64	0,065877	0,098717
128	0,037336	0,015387	128	0,037251	0,054298
256	0,019262	0,007987	256	0,019139	0,028635
512	0,008256	0,004118	512	0,009722	0,015150
1024	0,005072	0,002121	1024	0,004971	0,007823
2048	0,002598	0,001046	2048	0,002554	0,004020
4096	0,001328	0,000495	4096	0,001302	0,002069
8192	0,000650	0,000227	8192	0,000664	0,001062
16384	0,000295	0,000097	16384	0,000325	0,000524
32768	0,000126	0,000045	32768	0,000148	0,000247
65536	0,000044	0,000023	65536	0,000063	0,000114
131072	0,000027	0,328165	131072	0,000022	0,000048
			262144	0,000013	0,000022

Considere, por exemplo, $N = 1024$. Nos dois períodos considerados, há sucesso nos ensaios utilizando o entrelaçador BGL e falha quando o entrelaçador JPL é empregado. Entretanto, no caso do período T_1 , tem-se $\gamma_{BGL} > \gamma_{JPL}$, enquanto que no caso do período T_2 , tem-se $\gamma_{BGL} < \gamma_{JPL}$.

Considere agora os entrelaçadores TKC e WLC, que são considerados adequados para a aplicação, e possuem apenas fatores triviais de espalhamento, ou seja, possuindo parâmetro s unitário, o que implica em um fator λ muito próximo de zero quando o período é grande. À primeira vista, esse resultado leva a crer que se um entrelaçador possuir fatores triviais de espalhamento, então ele é adequado para ser aplicado nos esquemas de codificação homofônica. Considere agora o entrelaçador JPL, que não é adequado para a aplicação. Fazendo $T = 2^k$ e $N = 2^n$, esse entrelaçador também possui parâmetro s unitário quando $n \geq k - 5$, em que $k \geq 9$. Considere agora o entrelaçador BGL. Supondo $T = 2^k$ e $N = 2^n$, se $k \geq 17$ e $n \leq \left\lceil \frac{k}{2} \right\rceil + 1$, então ocorre aprovação nos testes estatísticos do NIST. Porém, para esse intervalo de n , o entrelaçador possui valores bem maiores que 1 para o parâmetro s . Para $T = 262144$ e $N = 1024$, por exemplo, tem-se $s = 255$, o que leva a $\lambda = 0,001945$ para o entrelaçador BGL, que é muito maior que $\lambda = 0,000008$, que é o fator λ associado aos entrelaçadores TKC e WLC para esse período. Logo, o espalhamento do entrelaçador não exerce influência na qualidade estatística da sequência de saída dos codificadores homofônicos OMI e DEI.

6.3 Análise do Codificador OMI/DEI com $n > 1$ (Ensaio 2)

Uma vez que foram identificados os entrelaçadores que apresentam problemas estatísticos no Ensaio 1, considere agora os casos em que os entrelaçadores BGL, TKC e WLC obtiveram sucesso em todas as fontes de informação. Fazendo $T = 2^k$, para o entrelaçador TKC, considere os 20 casos para $16 \leq k \leq 20$ (ver as Tabelas 6.3 e 6.4) e para o entrelaçador WLC, considere os 10 casos também para $16 \leq k \leq 20$ (ver a Tabela 6.5). No caso do entrelaçador BGL, os parâmetros relativos aos casos de sucesso estão listados na Tabela 6.7.

Tabela 6.7: Parâmetros associados aos casos de sucesso no Ensaio 1.

T	N								
65536	8	512							
131072	8	16	32	64	128	256	1024		
262144	8	16	32	64	128	256	512	1024	
524288	8	16	32	64	128	256	512	1024	2048
1048576	8	16	32	64	128	256	512	1024	2048

6.3.1 Objetivo e Metodologia do Ensaio 2

O objetivo do Ensaio 2 é investigar e comparar o comportamento estatístico dos codificadores OMI e DEI quando $n \geq 2$, ou seja, quando taxas maiores que $\frac{1}{2}$ são empregadas. Foram realizados 27750 ensaios, variando a memória n do codificador no intervalo $2 \leq n \leq 16$. Nos casos em que os entrelaçadores TKC e WLC são empregados, o critério de aceitação para uma determinada taxa é que pelo menos 75% dos casos analisados obtenham sucesso nos testes estatísticos. Assim, 15 casos precisam obter sucesso quando o entrelaçador TKC é empregado e pelo menos 8 casos precisam obter sucesso quando o entrelaçador WLC é empregado.

6.3.2 Resultados Envolvendo o Entrelaçador BGL

Os resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI estão ilustrados na Figura 6.16 e quando ele é empregado no codificador DEI estão ilustrados na Figura 6.17. Observando as figuras, percebe-se que os dois esquemas de codificação homofônica conseguem atingir a taxa $R = \frac{16}{17} = 0,9412$, porém com o codificador DEI consegue-se atingir essa taxa com um período menor no entrelaçador (utiliza menos memória em sua implementação). Note também que o número de falhas nos testes estatísticos para o codificador DEI é menor do que no caso do codificador OMI. Isso indica que, ao utilizar o entrelaçador BGL, a estrutura do codificador diferencial é mais eficiente do que a estrutura da cifra de blocos descartáveis para realizar codificação homofônica universal. Os resultados dos ensaios envolvendo as outras fontes de informação estão no Apêndice B.

OMI

I _N - Branco - BGL		
T = 65536		
n	N	
	8	512
1	97,87%	97,34%
2	97,87%	97,87%
3	98,94%	99,47%
4	97,87%	97,87%
5	96,81%	96,28%
6	93,62%	92,02%
7	88,30%	88,83%
8	87,77%	87,77%
9	82,98%	85,64%
10	82,45%	79,79%
11	80,85%	73,40%
12	74,47%	65,96%
13	67,55%	62,77%
14	68,09%	56,91%
15	66,49%	55,32%
16	60,64%	54,79%

I _N - Branco - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	97,87%	97,87%	97,87%	96,81%	96,81%	97,34%	96,81%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
5	95,74%	95,21%	95,21%	96,81%	95,74%	96,28%	95,74%
6	92,55%	95,21%	93,09%	95,21%	94,68%	92,02%	93,62%
7	88,30%	88,30%	88,83%	88,30%	87,77%	88,83%	87,77%
8	87,77%	87,23%	87,23%	87,23%	87,23%	88,83%	85,64%
9	86,17%	84,04%	82,98%	86,17%	84,57%	85,64%	83,51%
10	85,11%	84,04%	80,85%	81,91%	84,04%	81,38%	80,85%
11	81,91%	78,72%	79,79%	75,53%	80,85%	79,28%	72,34%
12	75,53%	70,21%	76,60%	76,60%	74,47%	72,34%	71,28%
13	73,94%	70,74%	68,62%	70,74%	68,62%	70,74%	60,64%
14	67,02%	65,96%	68,09%	64,89%	68,09%	66,49%	57,98%
15	62,77%	63,83%	62,23%	64,89%	67,55%	62,23%	53,72%
16	62,77%	62,77%	63,83%	60,11%	61,70%	61,70%	55,32%

I _N - Branco - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,81%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
3	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4	97,87%	97,34%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%
5	97,87%	97,87%	97,87%	97,87%	97,87%	96,28%	96,81%	96,81%
6	97,87%	96,28%	97,87%	97,87%	96,28%	95,74%	97,87%	96,28%
7	94,15%	96,28%	94,68%	95,74%	97,87%	95,21%	93,09%	92,55%
8	96,81%	94,15%	94,15%	94,68%	96,28%	94,15%	94,68%	90,43%
9	93,09%	94,68%	96,28%	93,62%	93,09%	93,62%	91,62%	88,30%
10	92,55%	94,15%	91,49%	94,15%	93,09%	93,09%	91,49%	86,70%
11	89,69%	88,83%	91,49%	89,36%	92,02%	89,36%	88,30%	81,91%
12	88,30%	89,36%	88,83%	87,23%	88,83%	89,36%	87,23%	79,28%
13	86,70%	86,17%	86,17%	88,83%	86,17%	84,04%	86,17%	73,94%
14	85,11%	85,11%	86,70%	85,64%	85,64%	86,70%	86,17%	74,47%
15	84,04%	82,98%	84,04%	84,57%	86,17%	82,45%	84,57%	70,21%
16	84,04%	82,45%	84,57%	83,51%	80,85%	82,45%	81,91%	65,96%

I _N - Branco - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
2	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
4	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%	97,87%	96,81%	
5	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	
6	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,13%	
7	97,34%	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%	97,34%	91,49%
8	97,87%	97,87%	96,28%	97,87%	97,87%	96,81%	96,81%	88,30%	
9	97,87%	97,87%	97,87%	97,87%	97,87%	96,81%	92,55%	89,36%	
10	97,87%	97,34%	96,81%	97,87%	97,87%	94,68%	96,28%	91,49%	85,11%
11	97,34%	95,74%	97,34%	96,81%	97,34%	96,28%	90,96%	81,91%	
12	96,28%	96,28%	96,28%	96,81%	95,74%	96,28%	95,21%	88,30%	82,45%
13	96,28%	95,74%	96,81%	94,68%	96,28%	95,74%	93,62%	89,89%	78,19%
14	94,68%	93,62%	93,62%	95,21%	95,21%	92,55%	93,62%	85,11%	70,74%
15	93,62%	91,49%	94,68%	93,62%	92,55%	90,96%	91,49%	84,57%	68,62%
16	91,49%	93,62%	93,62%	92,55%	92,02%	93,09%	94,15%	84,57%	63,83%

I _N - Branco - BGL										
T = 1048576										
n	N									
	8	16	32	64	128	256	512	1024	2048	
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%
5	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
6	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%
7	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	96,28%
8	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%	93,62%
9	96,81%	97,34%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	95,21%
10	97,34%	97,34%	96,81%	97,34%	96,28%	97,34%	97,34%	97,87%	97,87%	94,68%
11	97,34%	96,81%	97,87%	97,34%	96,81%	97,87%	96,81%	97,87%	96,81%	90,96%
12	97,34%	97,34%	96,28%	97,34%	97,87%	97,34%	96,28%	97,34%	97,34%	89,89%
13	97,34%	96,28%	96,81%	97,87%	96,81%	97,34%	97,34%	96,81%	96,81%	88,30%
14	97,87%	97,34%	97,34%	97,34%	96,81%	97,34%	96,81%	97,34%	96,81%	86,70%
15	96,81%	97,34%	97,34%	94,68%	95,74%	96,28%	97,87%	97,34%	97,34%	86,17%
16	96,28%	97,34%	96,81%	96,81%	96,81%	96,28%	94,68%	97,34%	97,34%	86,17%

Figura 6.16: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI.

DEI

I _N - Branco - BGL		
T = 65536		
n	N	
	8	512
1	97,87%	97,34%
2	97,34%	97,87%
3	97,34%	97,87%
4	96,81%	97,34%
5	97,34%	97,34%
6	96,81%	96,28%
7	97,34%	97,34%
8	97,87%	96,81%
9	96,81%	95,74%
10	97,87%	94,59%
11	97,87%	93,09%
12	97,34%	89,69%
13	97,87%	88,83%
14	97,34%	85,11%
15	88,83%	78,19%
16	97,34%	83,51%

I _N - Branco - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	97,87%	97,87%	97,87%	96,81%	96,81%	97,34%	96,81%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	97,87%	97,87%	97,87%	97,87%	96,81%	96,81%	97,87%
4	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
5	96,81%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
6	96,81%	96,81%	97,87%	97,87%	97,87%	97,87%	97,87%
7	97,02%	97,87%	97,34%	97,34%	97,34%	97,34%	97,87%
8	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	95,74%
9	96,81%	97,87%	96,28%	97,34%	97,87%	96,81%	94,68%
10	97,87%	97,34%	97,87%	97,87%	97,87%	97,34%	92,02%
11	97,87%	97,87%	97,34%	97,87%	97,34%	97,87%	92,02%
12	97,87%	97,87%	96,81%	97,87%	97,87%	97,34%	89,36%
13	97,34%	97,87%	97,34%	96,28%	97,87%	97,87%	88,83%
14	97,34%	97,87%	97,87%	97,87%	97,34%	97,87%	84,57%
15	89,36%	87,23%	97,34%	96,81%	96,81%	97,34%	81,38%
16	97,87%	97,34%	96,81%	97,87%	97,34%	96,81%	78,19%

I _N - Branco - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,81%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,34%	97,87%
4	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
5	96,81%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,34%
6	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
7	96,28%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
8	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
9	96,81%	97,87%	97,87%	97,34%	97,87%	96,81%	97,87%	97,87%
10	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
11	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%
12	97,34%	96,81%	97,87%	96,28%	97,87%	97,34%	97,87%	96,28%
13	97,87%	97,34%	97,87%	97,87%	97,87%	96,81%	97,87%	96,81%
14	97,87%	96,81%	97,87%	97,34%	97,34%	97,34%	97,87%	95,74%
15	96,28%	91,49%	97,87%	97,34%	97,34%	97,87%	97,34%	95,21%
16	97,34%	97,87%	96,28%	97,87%	97,87%	96,81%	97,34%	91,49%

I _N - Branco - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	96,81%
4	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
5	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	96,81%
6	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
7	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	96,81%
8	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,34%
9	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,34%	95,74%
10	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,34%	97,34%
11	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	96,28%	96,28%
12	97,87%	97,87%	96,81%	97,87%	97,87%	97,34%	97,34%	96,28%	96,28%
13	96,81%	97,87%	97,34%	97,87%	97,87%	97,34%	97,34%	92,55%	92,55%
14	97,87%	97,87%	97,34%	97,87%	97,87%	97,34%	97,87%	94,68%	94,68%
15	97,34%	97,87%	97,34%	97,87%	97,34%	97,34%	97,34%	91,49%	91,49%
16	96,28%	97,34%	97,34%	97,34%	97,34%	97,87%	97,34%	94,15%	94,15%

I _N - Branco - BGL										
T = 1048576										
n	N									
	8	16	32	64	128	256	512	1024	2048	4096
1	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
2	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
3	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
4	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
5	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
6	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
7	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%
8	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%
9	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%
10	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
11	97,87%	97,34%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,87%
12	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%
13	97,34%	96,81%	97,87%	97,34%	96,81%	97,87%	97,87%	97,87%	97,87%	97,87%
14	97,87%	97,87%	97,34%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%	97,34%
15	96,81%	97,34%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%
16	95,21%	97,87%	97,34%	97,87%	97,34%	97,87%	97,87%	97,34%	97,34%	97,34%

Figura 6.17: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI.

6.3.3 Resultados Envolvendo o Entrelaçador TKC

Os resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI estão ilustrados na Figura 6.18 e quando ele é empregado no codificador DEI estão ilustrados na Figura 6.19.

Observando a Figura 6.18, percebe-se que o codificador OMI atinge com segurança uma taxa $R = \frac{14}{15} = 0,9333$. A taxa $R = \frac{16}{17} = 0,9412$ é obtida para $T = 2^{20}$, mas como há 12 casos de falha quando esse período é utilizado (mais da metade), então não é considerado seguro esse cenário. No caso do codificador DEI (Figura 6.19), percebe-se que esse codificador atinge uma taxa $R = \frac{16}{17} = 0,9412$ com segurança, inclusive com uma quantidade bem menor de memória no entrelaçador ($T = 2^{16}$). Assim como no caso do entrelaçador BGL, a estrutura do codificador diferencial é mais eficiente do que a estrutura da cifra de blocos descartáveis para realizar codificação homofônica universal. Os resultados dos ensaios envolvendo as outras fontes de informação estão no Apêndice B.



Figura 6.18: Resultados do Ensaio 2 quando o entrelaçador TKC é empregado no codificador OMI.

6.3.4 Resultados Envolvendo o Entrelaçador WLC

Os resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI estão ilustrados na Figura 6.20 e quando ele é empregado no codificador DEI estão ilustrados na Figura 6.21.

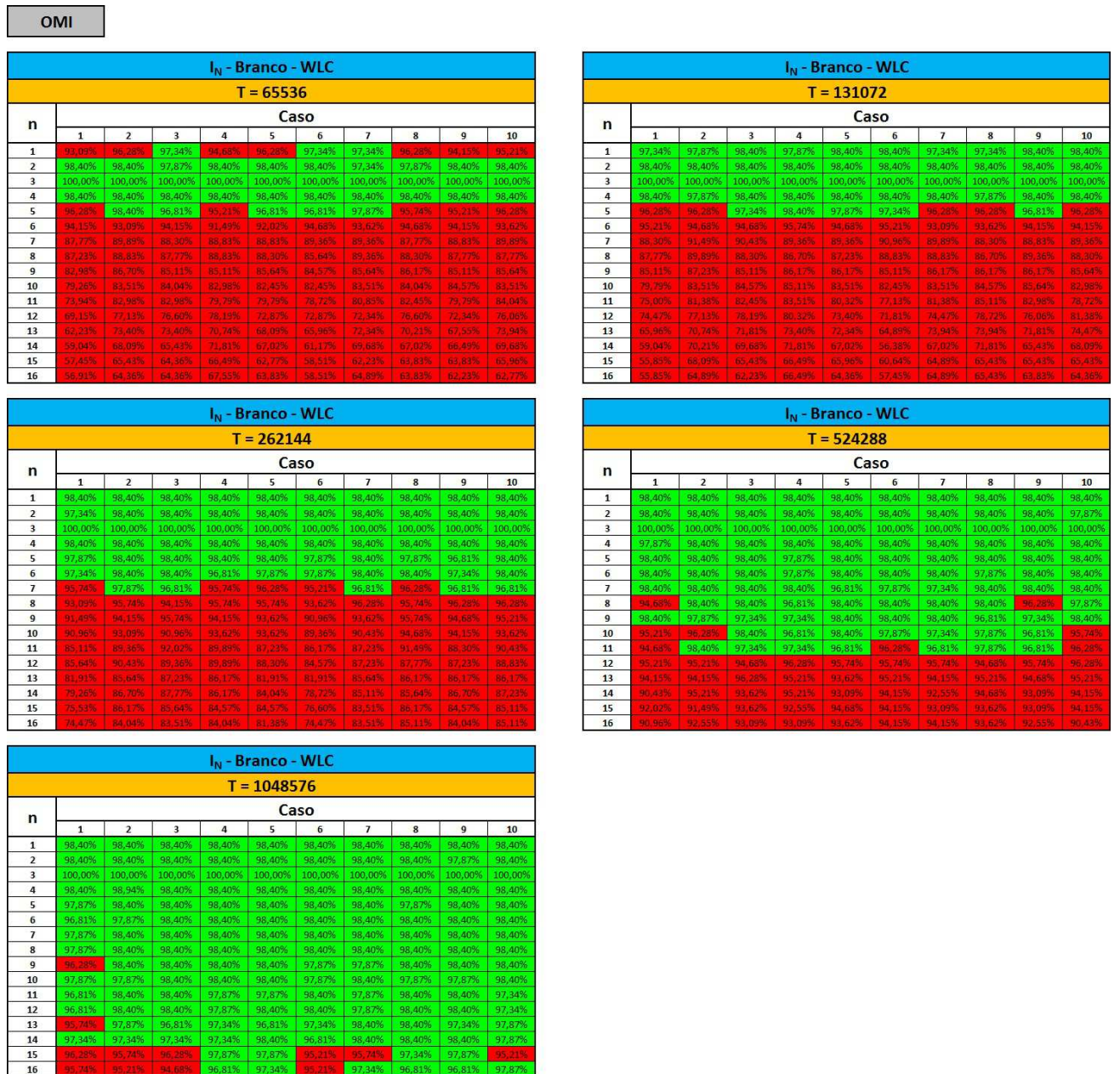


Figura 6.20: Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI.

DEI

I _N - Branco - WLC										
T = 65536										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	94,00%	96,26%	97,34%	98,68%	96,26%	97,34%	97,34%	96,26%	94,15%	95,21%
2	98,40%	98,40%	98,40%	97,34%	98,40%	97,34%	98,40%	98,40%	98,40%	98,40%
3	97,34%	97,87%	98,40%	97,34%	99,62%	95,74%	97,34%	97,34%	98,40%	96,81%
4	98,40%	98,40%	98,40%	98,40%	98,40%	98,28%	98,40%	98,40%	98,40%	98,40%
5	97,34%	96,81%	98,40%	97,87%	98,40%	96,81%	96,81%	98,40%	98,40%	98,40%
6	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	97,34%	98,40%
7	95,74%	98,40%	98,40%	97,34%	97,87%	95,74%	96,81%	98,40%	95,21%	96,81%
8	97,87%	98,40%	98,40%	98,40%	97,87%	97,34%	97,87%	98,40%	96,81%	98,40%
9	95,74%	97,87%	98,40%	97,34%	97,87%	94,68%	97,87%	97,34%	95,74%	94,74%
10	91,49%	98,40%	98,40%	98,40%	97,87%	95,74%	97,87%	98,40%	95,74%	97,87%
11	92,55%	97,34%	96,81%	98,40%	97,34%	97,34%	94,68%	98,40%	95,74%	98,40%
12	93,62%	98,40%	97,34%	97,87%	97,34%	95,74%	96,28%	96,81%	96,81%	97,87%
13	90,96%	96,81%	96,81%	97,34%	95,74%	95,21%	94,68%	97,34%	95,21%	97,87%
14	88,30%	98,40%	95,74%	96,81%	96,28%	94,68%	95,74%	96,28%	96,28%	98,40%
15	86,70%	97,87%	96,81%	96,81%	96,81%	93,09%	95,74%	94,15%	95,74%	98,40%
16	87,23%	97,87%	98,28%	97,87%	96,28%	94,15%	97,34%	95,74%	96,28%	98,40%

I _N - Branco - WLC										
T = 131072										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	97,34%	97,87%	98,40%	97,87%	98,40%	98,40%	97,34%	97,34%	98,40%	98,40%
2	98,40%	98,40%	97,34%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
3	97,87%	97,34%	98,40%	98,40%	96,81%	97,34%	98,40%	98,40%	98,40%	98,40%
4	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
5	97,34%	98,40%	98,40%	98,40%	98,40%	96,81%	98,40%	98,40%	98,40%	98,40%
6	97,34%	98,40%	97,87%	98,40%	98,40%	96,28%	98,40%	98,40%	97,87%	97,34%
7	97,34%	98,40%	98,40%	98,40%	98,40%	96,81%	97,87%	97,87%	97,34%	97,34%
8	96,81%	98,40%	97,34%	98,40%	97,87%	96,81%	98,40%	98,40%	97,34%	98,40%
9	92,02%	98,40%	98,40%	98,40%	97,87%	95,74%	98,40%	98,40%	97,34%	98,40%
10	94,68%	97,87%	97,34%	98,40%	97,87%	97,87%	98,40%	98,40%	97,87%	98,40%
11	91,49%	98,40%	98,40%	98,40%	96,81%	95,21%	98,40%	98,40%	96,81%	98,40%
12	93,62%	98,40%	98,40%	98,40%	97,87%	95,21%	96,81%	96,81%	97,34%	97,34%
13	87,77%	98,40%	97,34%	98,40%	97,87%	96,81%	98,40%	96,81%	97,87%	98,40%
14	87,23%	97,34%	97,34%	97,87%	97,87%	94,68%	98,40%	97,87%	96,81%	98,40%
15	87,77%	98,40%	98,40%	97,87%	97,34%	93,62%	96,81%	96,81%	96,81%	98,40%
16	87,77%	98,40%	97,34%	98,40%	96,81%	92,55%	97,34%	96,81%	96,81%	98,40%

I _N - Branco - WLC										
T = 262144										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
2	97,87%	97,87%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
3	97,34%	98,40%	98,40%	98,40%	98,40%	97,34%	98,40%	98,40%	98,40%	98,40%
4	97,87%	98,40%	96,81%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
5	97,34%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%
6	97,34%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%
7	97,34%	98,40%	98,40%	98,40%	97,34%	98,40%	97,87%	98,40%	98,40%	98,40%
8	97,87%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%
9	96,81%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%
10	95,21%	98,40%	98,40%	98,40%	97,87%	95,21%	97,87%	98,40%	98,40%	98,40%
11	95,74%	98,40%	98,40%	98,40%	97,87%	95,74%	96,81%	98,40%	98,40%	98,40%
12	94,68%	97,87%	98,40%	98,40%	97,87%	94,68%	97,87%	98,40%	98,40%	98,40%
13	95,74%	97,87%	98,40%	97,87%	97,87%	96,81%	97,87%	98,40%	97,87%	98,40%
14	95,74%	97,87%	98,40%	98,40%	97,87%	95,74%	97,87%	98,40%	98,40%	98,40%
15	94,68%	97,34%	98,40%	97,87%	97,87%	95,21%	97,87%	98,40%	98,40%	98,40%
16	94,15%	97,87%	98,40%	98,40%	96,28%	94,68%	97,34%	98,40%	98,40%	98,40%

I _N - Branco - WLC										
T = 524288										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
2	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
3	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
4	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
5	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
6	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
7	97,87%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%
8	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
9	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%
10	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
11	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
12	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
13	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
14	97,34%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
15	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
16	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%

I _N - Branco - WLC										
T = 1048576										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
2	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
3	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
4	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%
5	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
6	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
7	97,87%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	98,40%
8	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
9	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
10	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
11	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
12	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
13	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
14	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
15	97,87%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%
16	97,87%	98,40%	98,40%	98,40%	97,87%	97,87%	98,40%	98,40%	98,40%	97,34%

Figura 6.21: Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador DEI.

Observando a Figura 6.20, percebe-se que o codificador OMI atinge com segurança uma taxa $R = \frac{14}{15} = 0,9333$. A taxa $R = \frac{16}{17} = 0,9412$ é obtida para $T = 2^{20}$, mas como há 4 casos de falha quando esse período é utilizado, então também não é considerado seguro esse cenário. No caso do codificador DEI (Figura 6.21), percebe-se que esse codificador atinge uma taxa $R = \frac{16}{17} = 0,9412$ com segurança, inclusive com uma quantidade bem menor de memória no entrelaçador ($T = 2^{17}$). Os resultados desses ensaios confirmam mais uma vez a maior eficiência do codificador diferencial em relação à cifra de blocos descartáveis na codificação homofônica universal. Os resultados dos ensaios envolvendo as outras fontes de informação

estão no Apêndice B.

6.3.5 Comentários para o Ensaio 2

Os resultados apresentados para o Ensaio 2 mostram que tanto o codificador OMI quanto o codificador DEI atingem com sucesso a taxa $R = \frac{16}{17} = 0,9412$. No caso do codificador OMI, essa taxa só é atingida quando o entrelaçador BGL é empregado. Por outro lado, no caso do codificador DEI, essa taxa é atingida com o emprego de qualquer um dos três entrelaçadores considerados no ensaio, o que representa uma vantagem em relação ao codificador OMI.

Outra vantagem do codificador DEI em relação ao OMI é que ele necessita de bem menos memória no entrelaçador (período menor) para atingir taxas altas. A Tabela 6.8 mostra, para os dois esquemas de codificação homofônica, a taxa máxima atingida e o período necessário para cada entrelaçador, utilizando o critério de pelo menos 75% dos casos tendo sucesso para os entrelaçadores TKC e WLC. Esses resultados são conclusivos para evidenciar a maior eficiência do codificador diferencial em relação à cifra de blocos descartáveis quando ele é aplicado no esquema de codificação homofônica universal.

Tabela 6.8: Taxas atingidas e período requerido (entrelaçador) para os esquemas de codificação homofônica universal OMI e DEI.

Entrelaçador	Taxa Máxima		Período Requerido	
	OMI	DEI	OMI	DEI
BGL	0,9412	0,9412	1048576	65536
TKC	0,9333	0,9412	1048576	65536
WLC	0,9333	0,9412	1048576	131072

Os resultados apresentados para o Ensaio 2 não são exaustivos, pois os dois esquemas de codificação homofônica universal apresentaram indícios de que podem trabalhar eficientemente com taxas ainda maiores.

CAPÍTULO 7

CONCLUSÕES

Esta tese apresenta uma análise detalhada dos codificadores homofônicos universais OMI e DEI, considerando diversos entrelaçadores paramétricos em sua implementação. Essas técnicas tornam os cripto-sistemas simétricos não expansivos fortemente ideais, segundo o conceito de Shannon, sem necessitar do conhecimento *a priori* da estatística da fonte de informação. Os codificadores homofônicos analisados possuem implementação simples e são bastante atraivos em aplicações práticas. Além disso, conseguem atingir taxas altas, pelo menos 0,9412 para o pior caso (fonte de entropia zero) e possuem uma eficiência estatística satisfatória, como é demonstrado em um total de 37500 ensaios estatísticos realizados, envolvendo fontes de informação e parâmetros diferentes, utilizando uma versão otimizada da suíte de testes do NIST, e um critério alternativo ao que foi adotado para testar os cripto-sistemas candidatos a se tornar o padrão AES. Constata-se também uma melhor eficiência do codificador DEI em relação ao codificador OMI, necessitando de menos memória no entrelaçador para atingir as taxas elevadas.

Alguns dos entrelaçadores considerados apresentam defeitos estatísticos, que foram detectados nos ensaios, sendo classificados como inapropriados para serem aplicados nos esquemas de codificação homofônica universal. Constata-se que o período é o parâmetro do entrelaçador que mais exerce influência na qualidade estatística da sequência de saída dos codificadores homofônicos. Além disso, expressões paramétricas para os cálculos de dispersão e espalhamento do entrelaçadores são apresentados, servindo como ponto inicial para encontrar expressões generalizadas para esses parâmetros. No caso da dispersão, uma definição alternativa é apresentada, que permite o seu cálculo de forma paralela e também uma representação em função

das possíveis diferenças dos índices temporais da sequência de entrada.

7.1 Sugestões para Trabalhos Futuros

Os ensaios para a investigação das taxas máximas que os codificadores conseguem atingir não foram exaustivos, havendo potencial para a confirmação de uma codificação homofônica com taxas ainda maiores nos dois esquemas. Outros entrelaçadores podem ainda ser considerados, uma vez que tenham propriedades interessantes para a aplicação. Outro aspecto que merece uma investigação é considerar o impacto de defeitos na geração dos números pseudo-aleatórios na qualidade estatística da sequência de saída dos codificadores, ou seja, supondo um gerador que emita zeros e uns com probabilidade p e $1 - p$, em que $p \neq \frac{1}{2}$.

Pode-se investigar ainda o comportamento desses esquemas com um outro elemento difusor no lugar do entrelaçador. Sugere-se uma abordagem envolvendo um registrador realimentado de deslocamento realizando esse papel. Outra sugestão para trabalhos futuros é a continuação da investigação das propriedades dos entrelaçadores para encontrar expressões parametrizadas gerais para a dispersão e o espalhamento e, indo além, expressões parametrizadas para os vetores de deslocamento, em função de Δ_x .

BIBLIOGRAFIA

- [1] S. Singh, *The Code Book - The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, 1999.
- [2] E. Lerville, *Les Cahiers Secrets de la Cryptographie*, Editions du Rocher, 1972.
- [3] C. Günther, “A Universal Algorithm for Homophonic Coding”, *Advances in Cryptology - Eurocrypt '88*, (Ed. C.G.Günther) LNCS, Springer-Verlag, No. 330, pp. 405-41, 1988.
- [4] H. K. Jendal, Y. J. B. Kuhn e J. L. Massey, “An Information-Theoretic Approach to Homophonic Substitution”, *Advances in Cryptology - Eurocrypt '89*, (Eds. J.-J. Quisquater e J.Vanderwalle), Lect. Notes in Comp. Sci., No. 434, Springer, pp 382-394, 1990.
- [5] V. C. da Rocha Jr. e J. L. Massey, “Better than “Optimum” Homophonic Substitution”, *Proc. IEEE International Symposium on Information Theory*, p. 241, Sorrento, Itália, 2000.
- [6] V. C. da Rocha Jr., “Perfect Homophonic Substitution with Finite Memory”, *Proc. IEEE International Symposium on Information Theory*, p. 409, Lausanne, Suíça, 2002.
- [7] J. L. Massey, “Some Applications of Source Coding in Cryptography”, *European Transactions on Telecommunications*, Vol.5, No. 4, pp. 421-429, 1994.
- [8] D. R. Simões, “Uma Nova Proposta para a Codificação Homofônica Universal”, *Dissertação de Mestrado*, PPGEE/UFPE, 2009.
- [9] D. R. Simões e V. C. da Rocha Jr., “A Versatile Scheme of Homophonic Coding”, *X International Symposium on Communication Theory and Applications - ISCTA '09*, Ambleside, Inglaterra, 2009.
- [10] D. R. Simões, J. Portugheis e V. C. da Rocha Jr., “Codificação Homofônica Universal Utilizando Codificação Diferencial e Entrelaçamento”, *XXVII Simpósio Brasileiro de Telecomunicações*, Blumenau - SC, Brasil, 2009.

- [11] D. R. Simões, J. Portugheis e V. C. da Rocha Jr., “Universal Homophonic Coding Scheme Using Differential Encoding and Interleaving”, *Information Processing Letters*, Volume 113(17), pp. 628-633, 2013.
- [12] A. Rukhin et al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” National Institute of Standards and Technology, Special Publication 800-22, Revision 1a, 2010, disponível *on-line*: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf>. Acesso em Outubro de 2017.
- [13] C. Berrou, A. Glavieux e P. Thitimajshima, “Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes”, *Proceedings of the IEEE International Conference on Communications*, pp. 1064-1070, Genebra, Suíça, 1993.
- [14] C. Berrou e A. Glavieux, “Near Optimum Error Correcting Coding and Decoding: Turbo-Codes”, *IEEE Transactions on Communications*, 44(10), pp. 1261-1271, 1996.
- [15] S. Dolinar, D. Divsalar e F. Pollara, “Code Performance as a Function of Block Size”, *TMO Progress Report 42-133*, JPL, Maio, 1998.
- [16] O. Y. Takeshita e D. J. Costello Jr., “New Classes of Algebraic Interleavers for Turbo-Codes”, *Proc. International Symposium on Information Theory*, pp. 419, Agosto, 1998.
- [17] J. P. Costas, “Medium Constraints on Sonar Design and Performance”, *EASCON Convention Record*, pp. 68A-68L, 1975.
- [18] M. Sýs, Z. Ríha e V. Matyás, “Algorithm 970: Optimizing the NIST Statistical Test Suite and the Berlekamp-Massey Algorithm”, *ACM Transactions on Mathematical Software*, Vol. 43, No. 3, Artigo 27, 2016.
- [19] K. Park e Keith W. Miller, “Random Number Generators: Good Ones are Hard to Find”, *Communications of ACM*, Vol. 31, No. 10, 1988.
- [20] David G. Carta, “Two Fast Implementations of the “Minimal Standard” Random Number Generator”, *Communications of ACM*, Vol. 33, No. 1, 1990.
- [21] C. Heegard e S. B. Wicker, *Turbo Coding*. Kluwer Academic Publishers, 1999. ISBN 0-7923-8378-8.

- [22] C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell Sys. Tech. J.*, Vol. 28, pp. 656-715, 1949.
- [23] N. Abramson, *Information Theory and Coding*. McGraw-Hill, 1963. ISBN 0-0700-0145-6.
- [24] T. J. Lynch, "Sequence Time Coding for Data Compression", *Proceedings of the IEEE (Lett.)*, Vol. 54, pp. 1490-1491, 1966.
- [25] L. D. Davisson, "Comments on 'Sequence Time Coding for Data Compression'", *Proceedings of the IEEE (Lett.)*, Vol. 54, p. 2010, 1966.
- [26] P. Elias, "Universal Codeword Sets and Representations of the Integers", *IEEE Transactions on Information Theory*, Vol. IT-21, pp. 194-203, 1975.
- [27] P. Elias, "Interval and Recency Rank Coding: Two On-Line Adaptative Variable-Length Schemes", *IEEE Transactions on Information Theory*, Vol. IT-33, pp. 3-10, 1987.
- [28] F. M. J. Willems, "Universal Data Compression and Repetition Times", *IEEE Transactions on Information Theory*, Vol. IT-35, pp. 54-58, 1989.
- [29] J. Ziv e A. Lempel, "A Universal Algorithm for Sequential Data Compression", *IEEE Trans. Inform. Th.*, Vol. IT-23, pp. 337-343, 1977.
- [30] J. Ziv e A. Lempel, "Compression of Individual Sequences via Variable-Rate Coding", *IEEE Trans. Inform. Th.*, Vol. IT-24, No. 5, pp. 5306, 1978.
- [31] T. A. Welch, "A Technique for High Performance Data Compression", *IEEE Computer*, Vol. 17, pp. 8-19, 1984.
- [32] D. R. Simões e V. C. da Rocha Jr., "Um Esquema de Codificação Homofônica Universal Utilizando o Algoritmo LZW", *XXVI Simpósio Brasileiro de Telecomunicações*, Rio de Janeiro - RJ, Brasil, 2008.
- [33] D. R. Simões e V. C. da Rocha Jr., "Investigação de Entrelaçadores para Aplicação em Codificação Homofônica Universal", *XXXIV Simpósio Brasileiro de Telecomunicações*, Santarém - PA, Brasil, 2016.
- [34] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997. ISBN 0-8493-8523-7.

- [35] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Wiley & Sons, 1996. ISBN 0-4711-2845-7.
- [36] D. E. Knuth, *The Art of Computer Programming - Seminumerical Algorithms*, Vol. 2, Addison-Wesley, 3a. Edição, Reading, Massachusetts, 1997. ISBN 0-201-89684-2.
- [37] J. B. Plumstead, "Inferring a sequence generated by a linear congruence", *Proceedings of the IEEE 23rd Annual Symposium on Foundations of Computer Science*, pp. 153-159, 1982.
- [38] J. Boyar, "Inferring sequences produced by pseudo-random number generators", *Journal of the Association for Computer Machinery*, 36, pp. 129-141, 1989.
- [39] H. Krawczyk, "How to predict congruential generators", *Advances in Cryptology - CRYPTO '89* (LNCS 435), pp. 138-153, 1990.
- [40] Lehmer D. H., "Mathematical Methods in Large-Scale Computing Units", *Annu. Comput. Lab. Harvard Univ.*, No. 26, pp. 141-146, 1951.
- [41] David M. Burton, *Elementary Number Theory*, McGraw-Hill, 6a Edição, 2007. ISBN 978-0-07-305188-8.
- [42] P. A. Lewis, A. S. Goodman, J. M. Miller, "A Pseudo-Random Number Generator for the System/360", *IBM Syst.*, J. 8, pp. 136-146, 1969.
- [43] G. S. Fishman e L. R. Moore, "An Exhaustive Analysis of Multiplicative Congruential Random Number Generators With Modulus $2^{31} - 1$ ", *SIAM J. Sci. Stat. Comput.*, Vol. 7, pp. 24-45, 1986.
- [44] L. Schrage, "A More Portable FORTRAN Random Number Generator", *ACM Trans. Math. Softw.*, Vol. 5, pp. 132-138, 1979.
- [45] G. R. Brown, *Dieharder: A Random Number Test Suite*, Version 3.31.1, 2004, disponível on-line em <http://webhome.phy.duke.edu/~rgb/General/dieharder/>. Acesso em Outubro de 2017.
- [46] P. L'Ecuyer e R. Simard, "A C Library for Empirical Testing of Random Number Generators", *ACM Transactions on Mathematical Software*, Vol. 33, No. 4, Artigo 22, 2007.

- [47] J. Walker, *ENT - A Pseudorandom Number Sequence Test Program*, 2008, disponível *on-line* em <http://www.fourmilab.ch/random/>. Acesso em Outubro de 2017.
- [48] H. Gustafson, E. Dawson, L. Nielsen e W. Caelli, “A Computer Package for Measuring the Strength of Encryption Algorithms”, *Computers & Security*, Vol. 13, pp. 687-697, 1994.
- [49] J. Soto e L. Bassham, “Randomness Testing of the Advanced Encryption Standard Finalist Candidates”, Computer Security Division, National Institute of Standards and Technology, 2000.
- [50] M. Sýs et al., “On the Interpretation of Results from the NIST Statistical Test Suite”, *Romanian Journal for Information Science and Technology (ROMJIST)*, Vol. 18, No. 1, 2015.
- [51] *The USC-SIPI Image Database, University of Southern California*, disponível *on-line* em <http://sipi.usc.edu/database/>. Acesso em Outubro de 2017.

APÊNDICE A

GERADOR DE PARK-MILLER-CARTA - ABORDAGEM TEÓRICA

Aborda-se aqui a teoria envolvida nas três questões citadas na Seção 2.4, utilizadas para encontrar um multiplicador a com propriedades de interesse. Considere inicialmente a questão Q_1 , o teste de periodicidade máxima. Para um bom entendimento desse teste, são necessários alguns conhecimentos sobre Teoria dos Números. A seguir, são apresentadas algumas definições e teoremas, sem mostrar as respectivas provas, extraídos de [41]:

Teorema A.1 (O Pequeno Teorema de Fermat) *Seja p um número primo e suponha que $p \nmid a$. Então $a^{p-1} \equiv 1 \pmod{p}$.*

Definição A.1 (A Função Phi de Euler) *Para um número inteiro $n \geq 1$, seja $\phi(n)$ o número de inteiros positivos de 1 a n que são relativamente primos com n .*

Teorema A.2 *A função ϕ é multiplicativa, ou seja, $\phi(mn) = \phi(m)\phi(n)$, sempre que $\text{mdc}(m, n) = 1$.*

Teorema A.3 *Se o número inteiro $n > 1$ possui a fatoração prima $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, então*

$$\phi(n) = n \prod_{i=1}^r \left[\frac{p_i - 1}{p_i} \right].$$

Definição A.2 (Ordem de um número inteiro módulo n) *Sejam os números inteiros $n > 1$ e a , tais que $\text{mdc}(a, n) = 1$. A ordem de a módulo n é o menor número inteiro positivo k tal que $a^k \equiv 1 \pmod{n}$.*

Teorema A.4 *Seja o número inteiro a possuindo ordem k módulo n . Então $a^h \equiv 1 \pmod{n}$ se e somente se $k \mid h$; em particular, $k \mid \phi(n)$.*

Teorema A.5 *Se o número inteiro a possui ordem k módulo n e $h > 0$, então a^h possui ordem $\frac{k}{\text{mdc}(h, k)}$ módulo n .*

Definição A.3 (Raiz primitiva) *Sejam a e n números inteiros. Se $\text{mdc}(a, n) = 1$ e a possui ordem $\phi(n)$ módulo n , então a é uma raiz primitiva do número inteiro n .*

Teorema A.6 *Se o número inteiro n possuir raiz primitiva, então existem exatamente $\phi(\phi(n))$ raízes.*

Voltando à questão Q_1 (teste de periodicidade) mencionada anteriormente, tomando as Equações (3.4) e (3.5) e utilizando a semente inicial x_1 , chega-se aos seguintes resultados:

$$\begin{aligned} x_2 &\equiv ax_1 \pmod{p}, \\ x_3 &\equiv ax_2 \equiv a^2x_1 \pmod{p}, \\ x_4 &\equiv ax_3 \equiv a^3x_1 \pmod{p}, \\ &\vdots \end{aligned}$$

O que leva a

$$x_{n+1} \equiv a^n x_1 \pmod{p}, \quad n = 1, 2, 3, \dots \quad (\text{A.1})$$

Seja T o menor valor de n tal que a sequência se repita, ou seja, $x_{T+1} = x_1$. De (A.1), tem-se:

$$\begin{aligned} x_{T+1} &\equiv a^T x_1 \pmod{p}, \\ x_{T+1} &\equiv x_1 \pmod{p}, \\ a^T &\equiv 1 \pmod{p}. \end{aligned}$$

A existência de $T \leq p - 1$ é garantida pelo Pequeno Teorema de Fermat (Teorema A.1), pois, segundo este teorema, tem-se $a^{p-1} \equiv 1 \pmod{p}$.

Do fato de que $x_{T+1} = x_1$ tem-se:

$$\begin{aligned} x_{T+2} &\equiv a^{T+1}x_1 \equiv a^T a x_1 \equiv a x_1 \equiv x_2 \pmod{p}, \\ x_{T+3} &\equiv a^{T+2}x_1 \equiv a^T a^2 x_1 \equiv a^2 x_1 \equiv x_3 \pmod{p}, \\ x_{T+4} &\equiv a^{T+3}x_1 \equiv a^T a^3 x_1 \equiv a^3 x_1 \equiv x_4 \pmod{p}, \\ &\vdots \end{aligned}$$

O que leva a

$$x_{T+n} \equiv x_n \pmod{p}, \quad \forall n \geq 1. \quad (\text{A.2})$$

Desta forma, se $T = p - 1$, ou seja, se a é uma raiz primitiva de p , então $f(\cdot)$ é um gerador de período máximo. Por outro lado, se a não for uma raiz primitiva de p , então $f(\cdot)$ não é um gerador de período máximo e o período $T < p - 1$, que é a ordem de a módulo p , deve, de acordo com o Teorema A.4, dividir $\phi(p) = p - 1$, uma vez que p é primo. Por exemplo, para $p = 17$, tem-se que $a = 5$ é uma raiz primitiva de 17, por isso a sequência gerada é de período 16 (período máximo); enquanto que $a = 8$ possui ordem $8 = \frac{(17-1)}{2}$ módulo 17, sendo a sequência gerada de período 8.

Considere agora o módulo escolhido $p = 2^{31} - 1 = 2.147.483.647$. Fatorando $p - 1$, obtém-se $p - 1 = 2.147.483.646 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$. Utilizando os Teoremas A.2, A.3 e A.6, tem-se:

$$\begin{aligned} \phi(\phi(2^{31} - 1)) &= \phi(2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331), \\ &= \phi(2) \cdot \phi(3^2) \cdot \phi(7) \cdot \phi(11) \cdot \phi(31) \cdot \phi(151) \cdot \phi(331), \\ &= 1 \cdot 6 \cdot 6 \cdot 10 \cdot 30 \cdot 150 \cdot 330, \\ &= 534600000. \end{aligned}$$

Assim, existem 534600000 raízes primitivas módulo $p = 2^{31} - 1$. A questão Q_1 é um filtro que elimina aproximadamente 75% dos multiplicadores possíveis. Seja $\chi(p)$ a menor raiz primitiva do número primo p . Tem-se, para o módulo escolhido, $\chi(2^{31} - 1) = 7$. Utilizando o teorema A.5, tem-se que um número inteiro a é uma raiz primitiva módulo p se e somente se $a \equiv 7^b \pmod{p}$, em que $\text{mdc}(b, p - 1) = 1$. Tomando o menor número inteiro maior do que 1 e relativamente primo com $p - 1$, tem-se $b = 5$. Assim, $a = 7^5 = 16807$ é uma raiz primitiva.

Esse foi o multiplicador adotado por Lewis, Goodman e Miller [19], definindo assim a função geradora de período máximo mostrada na Equação (3.7).

Voltando a atenção agora para a questão Q_2 , o teste de aleatoriedade, é conhecido o fato de que todos os geradores multiplicativos congruenciais de números aleatórios possuem um defeito que não pode ser removido simplesmente ajustando a semente inicial, o multiplicador ou o módulo. O problema consiste na natureza “cristalina” dos geradores multiplicativos. Considere a sequência de saída do gerador x_1, x_2, x_3, \dots . As k -uplas (x_1, x_2, \dots, x_k) , $(x_2, x_3, \dots, x_{k+1})$, \dots , dos valores de saída do gerador são vistas como pertencentes a um espaço de k dimensões. O problema é que todos os pontos pertencem a um número finito e relativamente pequeno de hiperplanos paralelos [?]. Alguns testes de aleatoriedade são baseados na análise da estrutura dos hiperplanos no espaço de dimensão k , para pequenos valores de k . Fishman e Moore [43] consideraram um multiplicador como ótimo se para $2 \leq k \leq 6$, tomando cada conjunto de hiperplanos paralelos, a distância euclidiana entre hiperplanos adjacentes não exceda a distância mínima realizável por mais de 25%. Assim, os 534,6 milhões de multiplicadores que respondem à questão Q_1 foram examinados, sendo identificados apenas 410 multiplicadores considerados ótimos [43]. O multiplicador $a = 16807$ não está na lista desses 410 multiplicadores ótimos, porém ainda possui um bom desempenho quando se relaxa um pouco o critério da distância de 25%. O motivo da escolha desse multiplicador é que ele responde simultaneamente às questões Q_1 e Q_3 .

Finalmente, considere a questão Q_3 referente à eficiência da implementação do gerador utilizando uma aritmética de 32 *bits*, utilizando o método de Schrage [44]. A idéia básica é construir um algoritmo para calcular $f(x) \equiv ax \pmod{p}$, de modo que todos os resultados intermediários sejam limitados por $p-1$. Os casos potenciais de *overflow* associados ao cálculo de $f(\cdot)$ ocorrem porque o produto ax é calculado antes da operação modular com p .

Esse *overflow* pode ser evitado simplesmente trocando a ordem dessas duas operações. Por exemplo, se fosse possível fatorar p como $p = aq$ para algum número inteiro q , resultaria em $f(x) \equiv ax \pmod{aq} \equiv a(x \pmod{q})$. Como o módulo p é um número primo, a fatoração não é possível. Assim, considere

$$p = aq + r, \tag{A.3}$$

em que

$$q = \left\lfloor \frac{p}{a} \right\rfloor \quad \text{e} \quad r \equiv p \pmod{a}. \tag{A.4}$$

A notação $\lfloor \cdot \rfloor$ denota a função piso. Se o resto r for pequeno, especificamente se $r < q$, esta

decomposição de p permite construir um algoritmo para calcular $f(x)$ sem produzir resultados intermediários maiores em magnitude do que $p - 1$. No caso de $a = 16807$ e $p = 2^{31} - 1$, tem-se $q = 127773$ e $r = 2836$. Dividindo ax por p , tem-se $ax = p \left\lfloor \frac{ax}{p} \right\rfloor + (ax \pmod{p})$. Assim, pode-se escrever

$$f(x) \equiv ax \pmod{p} = ax - p \left\lfloor \frac{ax}{p} \right\rfloor. \quad (\text{A.5})$$

Dividindo agora x por q , tem-se $x = q \left\lfloor \frac{x}{q} \right\rfloor + (x \pmod{q})$. Deste modo, tem-se

$$\begin{aligned} ax &= a \left[q \left\lfloor \frac{x}{q} \right\rfloor + (x \pmod{q}) \right], \\ &= \left\lfloor \frac{aqx}{q} \right\rfloor + ax \pmod{q}, \\ &= ax \pmod{q} + \left\lfloor \frac{x(p-r)}{q} \right\rfloor, \\ &= a(x \pmod{q}) - r \left\lfloor \frac{x}{q} \right\rfloor + \left\lfloor \frac{px}{q} \right\rfloor. \end{aligned} \quad (\text{A.6})$$

Substituindo (A.6) em (A.5), tem-se então

$$\begin{aligned} f(x) &= a(x \pmod{q}) - r \left\lfloor \frac{x}{q} \right\rfloor + \left\lfloor \frac{px}{q} \right\rfloor - p \left\lfloor \frac{ax}{p} \right\rfloor, \\ &= a(x \pmod{q}) - r \left\lfloor \frac{x}{q} \right\rfloor + p \left[\left\lfloor \frac{x}{q} \right\rfloor - \left\lfloor \frac{ax}{p} \right\rfloor \right]. \end{aligned}$$

Deste modo, chega-se a

$$f(x) = \gamma(x) + p\delta(x), \quad (\text{A.7})$$

em que

$$\begin{aligned} \gamma(x) &= a(x \pmod{q}) - r \left\lfloor \frac{x}{q} \right\rfloor, \\ \delta(x) &= \left\lfloor \frac{x}{q} \right\rfloor - \left\lfloor \frac{ax}{p} \right\rfloor. \end{aligned}$$

Se $r < q$, então, para x entre 1 e $p - 1$, os seguintes resultados são verdadeiros [19]:

1. $\delta(x)$ vale 0 ou 1;
2. Tanto $a(x \pmod{q})$ quanto $r \left\lfloor \frac{x}{q} \right\rfloor$ estão entre 0 e $p - 1$;
3. $|\gamma(x)| \leq p - 1$.

O item 1 é consequência do fato de que se x e y são números reais com $0 \leq x - y \leq 1$, então $\lfloor x \rfloor - \lfloor y \rfloor$ vale 0 ou 1. Pelo fato de que $1 \leq f(x) \leq p - 1$, segue de (A.7) que $\delta(x) = 0$ se e somente se $1 \leq \gamma(x) \leq p - 1$ e que $\delta(x) = 1$ se e somente se $-(p - 1) \leq \gamma(x) \leq -1$.

Assim, a idéia do método de Schrage [44] é que a operação que pode resultar em um *overflow* fica especificada conhecendo-se $\delta(x)$, que pode ser calculado a partir de $\gamma(x)$. Deste modo, em vez de calcular $f(x)$, calcula-se primeiramente $\gamma(x)$. Se $\gamma(x) > 0$, associa-se $f(x) = \gamma(x)$, senão, associa-se $f(x) = \gamma(x) + p$.

Para o caso implementado com $p = 2^{31} - 1$, pode-se tomar a condição $(p \bmod a) < \lfloor \frac{p}{a} \rfloor$ como a definição para a questão Q_3 . Park e Miller verificaram, por busca exaustiva, que, como o multiplicador $a = 16807$, 23093 multiplicadores respondem afirmativamente às questões Q_1 e Q_3 [19]. Porém, nenhum deles está na lista dos 410 multiplicadores ótimos, ou seja, responde afirmativamente à questão Q_2 utilizando o critério da distância de 25%. Como foi dito anteriormente, se esse critério for relaxado para uma distância de 30%, resultará que, entre os multiplicadores que respondem à questão, o multiplicador $a = 16807$ utilizado na implementação, torna-se apropriado para a aplicação considerada.

APÊNDICE B

OUTROS RESULTADOS DOS ENSAIOS ESTATÍSTICOS

B.1 Ensaio 1

As figuras listadas na Tabela B.1 apresentam os resultados do Ensaio 1, envolvendo o respectivo entrelaçador, considerando as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.

Tabela B.1: Figuras associadas aos testes estatísticos do Ensaio 1, envolvendo as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.

Entrelaçador	Figura
BGL	B.1
JPL	B.2
LRTB	B.3
CPR	B.4
TKC	B.5
WLC	B.6

I _N - Agatha - BGL		N																
T	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	64,36%	27,66%	25,53%	98,94%														
128	65,15%	64,36%	23,94%	20,74%	98,40%													
256	98,94%	99,47%	64,36%	20,21%	19,68%	99,47%												
512	100,00%	100,00%	98,40%	64,36%	19,68%	18,62%	99,47%											
1024	100,00%	100,00%	100,00%	98,94%	64,89%	19,15%	21,28%	99,47%										
2048	99,47%	100,00%	100,00%	100,00%	98,40%	64,36%	19,68%	20,21%	99,47%									
4096	100,00%	100,00%	100,00%	99,47%	100,00%	98,40%	64,36%	19,68%	19,15%	99,47%								
8192	98,94%	100,00%	100,00%	100,00%	100,00%	100,00%	98,40%	64,36%	19,15%	20,74%	99,47%							
16384	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	97,87%	64,36%	19,15%	22,34%	99,47%						
32768	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	64,89%	19,15%	19,68%	99,47%					
65536	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	64,36%	19,68%	20,21%	99,47%				
131072	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	97,34%	63,83%	19,68%	20,74%	99,47%			
262144	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,40%	64,36%	19,15%	21,81%	99,47%		
524288	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	98,40%	64,89%	18,62%	21,28%	98,94%	
1048576	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,40%	64,36%	19,15%	22,87%	99,47%

I _N - Cana51 - BGL		N																
T	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	63,83%	25,43%	11,77%	98,94%														
128	98,94%	63,83%	28,72%	12,77%	98,40%													
256	99,47%	97,87%	63,83%	25,53%	12,77%	99,47%												
512	100,00%	99,47%	97,34%	63,83%	26,06%	12,77%	99,47%											
1024	100,00%	100,00%	100,00%	97,34%	63,83%	25,00%	12,77%	99,47%										
2048	99,47%	100,00%	100,00%	100,00%	97,34%	63,83%	23,40%	12,77%	99,47%									
4096	100,00%	100,00%	100,00%	100,00%	99,47%	97,87%	63,83%	23,40%	12,77%	99,47%								
8192	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	97,34%	63,83%	27,66%	12,77%	99,47%							
16384	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	97,34%	63,83%	26,06%	12,77%	99,47%						
32768	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	97,34%	63,83%	28,72%	12,77%	99,47%					
65536	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	97,34%	63,83%	27,13%	12,77%	99,47%				
131072	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	97,87%	63,83%	26,06%	12,77%	99,47%				
262144	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	97,34%	63,83%	24,47%	13,77%	99,47%			
524288	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	97,34%	63,83%	27,66%	12,77%	99,47%	
1048576	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	96,81%	63,83%	25,53%	12,77%	99,47%

I _N - Platão - BGL		N																
T	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	95,74%	41,49%	16,49%	98,94%														
128	99,47%	86,17%	40,96%	16,49%	98,94%													
256	100,00%	99,47%	71,66%	39,36%	15,99%	100,00%												
512	100,00%	100,00%	98,94%	71,81%	40,43%	16,49%	100,00%											
1024	100,00%	100,00%	100,00%	99,47%	72,34%	43,09%	15,96%	100,00%										
2048	100,00%	100,00%	100,00%	100,00%	99,47%	72,87%	43,09%	15,43%	100,00%									
4096	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	71,81%	43,62%	15,43%	98,94%								
8192	99,47%	99,47%	99,47%	100,00%	100,00%	100,00%	99,47%	71,81%	43,62%	15,96%	100,00%							
16384	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	73,40%	43,62%	15,96%	100,00%						
32768	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	73,40%	44,15%	15,43%	100,00%					
65536	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	68,62%	44,15%	15,96%	100,00%				
131072	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	99,47%	70,21%	44,15%	15,96%	100,00%			
262144	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	99,47%	72,34%	44,68%	15,96%	100,00%			
524288	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	71,81%	44,15%	15,96%	100,00%		
1048576	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	70,21%	44,15%	15,96%	99,47%

I _N - SC06 - BGL		N																
T	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	65,43%	34,04%	15,43%	99,47%														
128	99,47%	64,89%	33,51%	13,30%	98,40%													
256	99,47%	98,94%	64,89%	32,98%	13,83%	99,47%												
512	100,00%	99,47%	99,47%	64,36%	32,98%	13,83%	99,47%											
1024	100,00%	100,00%	100,00%	98,94%	64,89%	32,98%	15,43%	99,47%										
2048	100,00%	100,00%	100,00%	99,47%	98,94%	64,36%	33,51%	15,43%	99,47%									
4096	100,00%	100,00%	100,00%	99,47%	100,00%	98,94%	64,36%	32,45%	14,36%	99,47%								
8192	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	63,83%	32,98%	14,89%	99,47%							
16384	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	63,83%	32,98%	15,43%	99,47%						
32768	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	64,89%	32,98%	15,96%	99,47%					
65536	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	98,94%	64,36%	32,98%	14,36%	99,47%				
131072	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	99,47%	64,89%	32,98%	14,89%	98,94%			
262144	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	64,89%	32,98%	14,36%	99,47%		
524288	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	64,36%	31,38%	14,36%	99,47%		
1048576	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	64,89%	32,45%	14,36%	99,47%

Figura B.1: Resultados do Ensaio 1 envolvendo o entrelaçador BGL.

I_N - Agatha - JPL

T	N																			
	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	98,40%	98,39%	18,82%	21,81%	20,21%	16,49%														
128	98,40%	98,40%	27,66%	22,34%	20,74%	18,09%	18,82%													
256	98,40%	98,40%	27,13%	17,55%	23,40%	22,34%	17,55%	15,43%												
512	99,47%	98,94%	26,06%	13,30%	18,09%	25,53%	21,81%	18,09%	17,02%											
1024	99,47%	98,94%	97,87%	10,64%	13,30%	19,68%	22,87%	21,81%	19,68%	15,96%										
2048	99,47%	99,47%	97,87%	97,34%	11,17%	12,23%	20,74%	23,40%	21,81%	19,15%	17,02%									
4096	98,94%	99,47%	99,47%	97,87%	97,34%	12,77%	13,30%	20,21%	22,34%	20,21%	19,15%	16,49%								
8192	99,47%	99,47%	99,47%	98,40%	97,87%	97,34%	12,23%	13,30%	20,21%	22,67%	21,28%	19,15%	17,55%							
16384	99,47%	99,47%	99,47%	98,40%	98,94%	97,87%	97,34%	12,23%	13,30%	20,74%	22,34%	20,74%	19,15%	17,55%						
32768	99,47%	99,47%	99,47%	99,47%	98,94%	98,40%	97,87%	97,34%	12,77%	13,30%	20,74%	22,87%	21,28%	18,09%	16,49%					
65536	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%	97,34%	97,34%	12,77%	11,70%	20,74%	22,34%	21,81%	13,83%	16,49%				
131072	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%	97,87%	96,81%	10,11%	13,30%	20,74%	22,87%	21,28%	18,62%	15,96%		
262144	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%	97,87%	97,34%	12,23%	13,30%	20,21%	25,53%	21,81%	18,62%	21,28%		
524288	99,47%	99,47%	99,47%	99,47%	99,47%	97,34%	99,47%	99,47%	98,94%	98,94%	97,34%	96,81%	12,23%	12,77%	20,21%	23,40%	20,21%	18,62%	22,34%	
1048576	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,40%	98,94%	97,34%	96,81%	12,23%	13,83%	20,21%	21,87%	22,34%	18,09%	26,60%

I_N - Cana51 - JPL

T	N																			
	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	97,87%	15,43%	17,55%	14,36%	13,83%	11,70%														
128	97,87%	98,40%	15,96%	13,83%	13,83%	13,83%	11,70%													
256	98,94%	98,40%	29,79%	14,36%	14,89%	14,89%	13,83%	11,70%												
512	99,47%	98,94%	29,79%	16,49%	13,30%	15,43%	14,36%	13,83%	11,70%											
1024	99,47%	98,94%	97,87%	17,02%	16,49%	14,89%	14,36%	14,36%	13,83%	11,70%										
2048	99,47%	99,47%	97,87%	97,87%	17,02%	16,49%	14,36%	14,36%	14,36%	13,83%	11,70%									
4096	99,47%	99,47%	99,47%	97,87%	97,87%	17,02%	17,02%	13,83%	14,89%	14,36%	13,83%	11,70%								
8192	99,47%	99,47%	99,47%	98,94%	97,87%	17,55%	19,68%	14,36%	14,36%	14,36%	14,36%	14,36%	11,70%							
16384	99,47%	98,94%	99,47%	99,47%	99,47%	97,87%	97,87%	21,81%	25,53%	14,36%	15,96%	15,96%	15,43%	11,70%						
32768	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	97,87%	97,87%	26,72%	30,32%	14,36%	13,30%	14,89%	15,43%	11,70%					
65536	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,87%	97,87%	36,17%	39,36%	13,83%	14,36%	13,30%	13,83%	11,70%				
131072	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,87%	97,87%	37,23%	37,23%	15,43%	14,36%	14,36%	13,83%	11,70%			
262144	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,87%	97,87%	38,36%	36,70%	13,83%	15,43%	13,83%	18,62%	11,70%		
524288	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%	99,47%	98,94%	99,47%	97,87%	97,87%	38,36%	36,17%	15,43%	15,43%	15,96%	13,83%	11,70%	
1048576	99,47%	98,94%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	97,87%	97,34%	31,91%	36,70%	15,43%	14,36%	15,96%	13,30%	11,17%

I_N - Platão - JPL

T	N																			
	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	98,40%	29,64%	30,12%	21,28%	15,96%	13,30%														
128	98,40%	98,94%	29,20%	17,02%	19,15%	15,43%	13,83%													
256	100,00%	98,94%	67,02%	17,55%	17,02%	21,28%	15,96%	14,36%												
512	100,00%	100,00%	61,70%	32,11%	18,62%	17,02%	21,28%	17,55%	13,83%											
1024	100,00%	100,00%	99,47%	40,43%	47,34%	15,15%	17,02%	21,81%	17,55%	13,83%										
2048	100,00%	100,00%	99,47%	99,47%	36,17%	51,08%	18,62%	18,09%	22,34%	17,55%	13,43%									
4096	100,00%	100,00%	98,94%	100,00%	99,47%	47,34%	60,11%	23,81%	17,02%	21,28%	16,49%	13,83%								
8192	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	55,85%	63,84%	21,28%	19,15%	21,81%	19,15%	13,30%							
16384	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	67,77%	61,70%	26,60%	17,55%	21,28%	17,55%	13,83%						
32768	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	72,34%	68,62%	33,51%	18,62%	18,62%	17,55%	13,83%					
65536	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	71,28%	71,28%	31,91%	18,09%	18,62%	17,55%	13,83%				
131072	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	71,81%	73,40%	30,32%	20,21%	17,02%	16,49%	13,83%			
262144	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	76,06%	77,66%	31,91%	22,34%	21,28%	19,68%	13,30%			
524288	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	73,40%	72,87%	34,57%	23,40%	23,94%	22,87%	11,61%		
1048576	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	70,74%	71,28%	30,85%	26,60%	27,66%	23,94%	14,36%

I_N - SC06 - JPL

T	N																			
	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
64	97,87%	18,49%	15,96%	16,49%	14,36%	11,70%														
128	97,87%	98,40%	19,68%	14,89%	15,96%	14,89%	12,23%													
256	98,94%	98,40%	35,11%	15,96%	15,96%	15,96%	14,89%	12,77%												
512	99,47%	98,94%	29,79%	24,47%	16,49%	15,96%	15,96%	14,89%	13,30%											
1024	99,47%	98,94%	98,40%	18,62%	27,13%	16,49%	15,43%	15,43%	14,89%	12,77%										
2048	99,47%	98,94%	97,87%	97,87%	20,21%	27,13%	16,49%	14,36%	17,02%	14,89%	13,46%									
4096	99,47%	99,47%	98,94%	97,34%	98,40%	22,34%	28,72%	16,49%	16,49%	16,49%	14,89%	11,70%								
8192	99,47%	99,47%	98,94%	99,47%	98,40%	21,81%	32,43%	15,43%	17,02%	15,96%	13,83%	13,30%								
16384	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	98,40%	23,60%	28,72%	15,96%	16,49%	16,49%	14,89%	12,77%						
32768	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	98,40%	24,47%	28,19%	16,49%	16,49%	16,49%	14,36%	12,77%						
65536	99,47%	99,47%	99,47%	99,47%	98,40%	99,47%	99,47%	98,40%	98,40%	23,94%	28,19%	16,49%	16,49%	15,96%	14,89%	12,23%				
131072	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,87%	98,40%	26,60%	27,66%	16,49%	16,49%	16,49%	14,36%	12,77%			
262144	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	97,87%	28,19%	28,19%	15,43%	16,49%	17,02%	14,89%	12,77%		
524288	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,87%	97,87%	28,72%	26,06%	17,55%	16,49%	17,55%	14,89%	11,70%	
1048576	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	97,34%	96,40%	30,21%	29,79%	16,49%	17,55%	17,02%	14,89%	12,77%

Figura B.2: Resultados do Ensaio 1 envolvendo o entrelaçamento JPL.

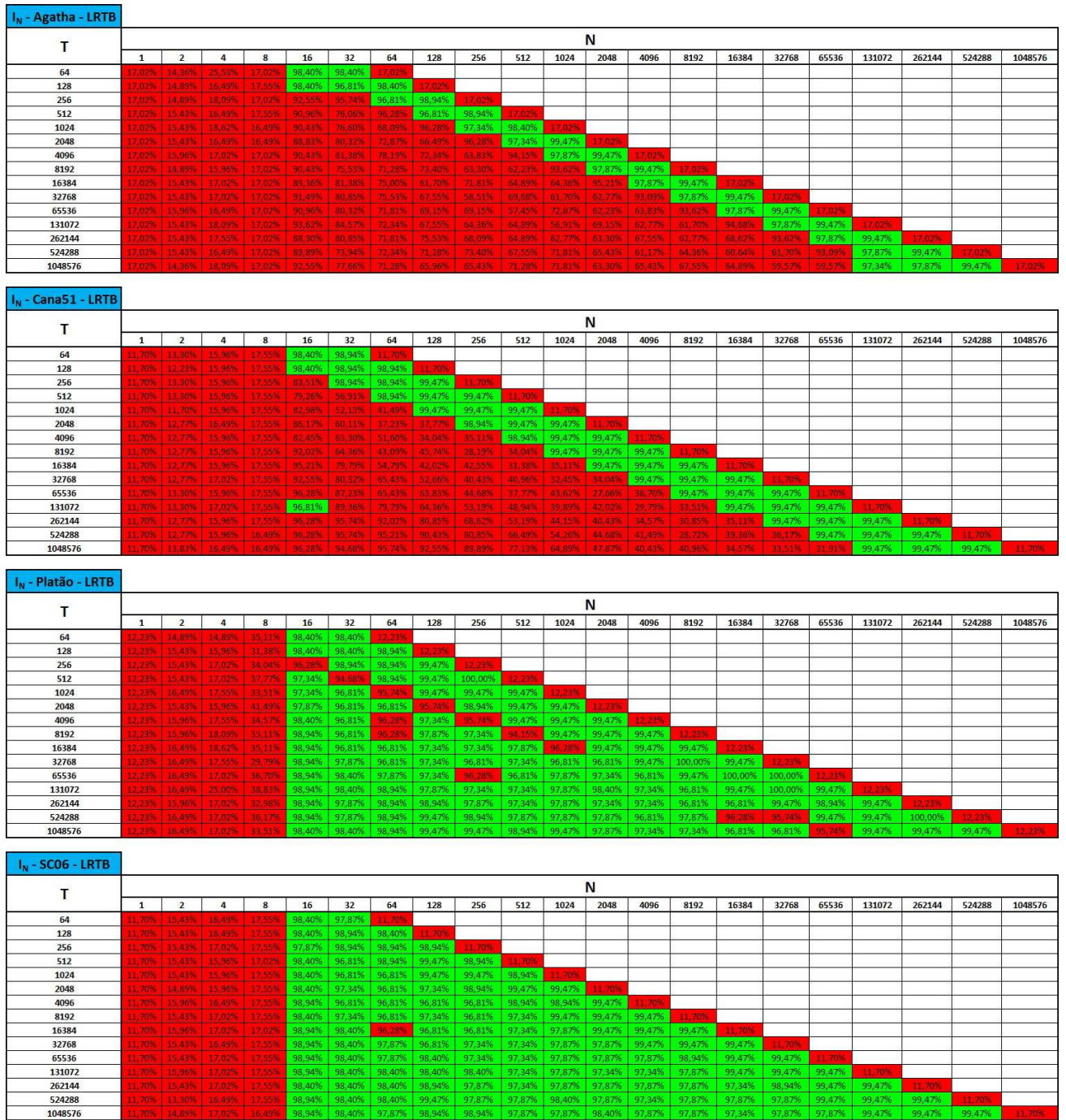


Figura B.3: Resultados do Ensaio 1 envolvendo o entrechador LRTB.

I _N - Agatha - WLC										
T	Caso									
	1	2	3	4	5	6	7	8	9	10
60	98,13%	92,96%	97,87%	97,87%	95,21%	83,51%	81,91%	93,62%	77,66%	95,21%
126	98,94%	97,34%	95,74%	94,15%	98,40%	97,34%	95,21%	98,40%	95,21%	98,94%
256	81,38%	86,70%	90,96%	88,30%	90,96%	88,30%	93,62%	91,49%	98,40%	80,85%
508	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
1020	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
2052	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4092	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	97,34%	100,00%	100,00%	100,00%
8190	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16380	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%
32770	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%
65536	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
131070	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
262146	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
524286	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
1048572	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - Cana51 - WLC										
T	Caso									
	1	2	3	4	5	6	7	8	9	10
60	77,66%	81,38%	90,43%	92,02%	87,77%	77,13%	80,32%	96,81%	70,74%	90,43%
126	99,47%	96,81%	95,21%	99,09%	97,87%	96,81%	92,96%	98,40%	94,68%	98,40%
256	90,43%	98,40%	97,87%	97,87%	93,62%	98,94%	97,87%	99,47%	98,94%	97,87%
508	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
1020	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
2052	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4092	100,00%	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	99,47%
8190	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
16380	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
32770	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
65536	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
131070	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
262146	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
524286	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
1048572	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - Platão - WLC										
T	Caso									
	1	2	3	4	5	6	7	8	9	10
60	94,15%	97,34%	99,47%	98,94%	99,47%	95,74%	97,87%	98,94%	96,81%	98,94%
126	99,47%	98,94%	98,94%	98,94%	99,47%	99,47%	98,94%	99,47%	98,94%	99,47%
256	98,94%	99,47%	98,94%	98,94%	98,94%	99,47%	99,47%	98,40%	99,47%	98,94%
508	99,47%	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%
1020	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%
2052	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4092	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8190	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16380	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
32770	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
65536	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
131070	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
262146	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
524286	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
1048572	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - SC06 - WLC										
T	Caso									
	1	2	3	4	5	6	7	8	9	10
60	71,81%	85,64%	95,21%	96,81%	98,94%	81,38%	85,64%	98,40%	81,91%	96,81%
126	99,47%	98,94%	98,94%	98,94%	99,47%	99,47%	98,94%	99,47%	97,34%	99,47%
256	97,87%	98,94%	98,40%	98,94%	98,40%	98,94%	99,47%	99,47%	99,47%	98,40%
508	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
1020	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
2052	98,94%	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	100,00%
4092	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	100,00%
8190	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16380	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
32770	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
65536	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
131070	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
262146	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
524286	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
1048572	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

Figura B.6: Resultados do Ensaio 1 envolvendo o entrelaçador WLC.

B.2 Ensaio 2

As figuras listadas na Tabela B.2 apresentam os resultados do Ensaio 2, envolvendo o respectivo entrelaçador, considerando as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.

Tabela B.2: Figuras associadas aos testes estatísticos do Ensaio 2, envolvendo as fontes de informação “Agatha”, “Cana51”, “Platão” e “SC06”.

Fonte	Codificador Homofônico	Entrelaçador	Figura
“Agatha”	OMI	BGL	B.7
“Agatha”	DEI	BGL	B.8
“Cana51”	OMI	BGL	B.9
“Cana51”	DEI	BGL	B.10
“Platão”	OMI	BGL	B.11
“Platão”	DEI	BGL	B.12
“SC06”	OMI	BGL	B.13
“SC06”	DEI	BGL	B.14
“Agatha”	OMI	TKC	B.15
“Agatha”	DEI	TKC	B.16
“Cana51”	OMI	TKC	B.17
“Cana51”	DEI	TKC	B.18
“Platão”	OMI	TKC	B.19
“Platão”	DEI	TKC	B.20
“SC06”	OMI	TKC	B.21
“SC06”	DEI	TKC	B.22
“Agatha”	OMI	WLC	B.23
“Agatha”	DEI	WLC	B.24
“Cana51”	OMI	WLC	B.25
“Cana51”	DEI	WLC	B.26
“Platão”	OMI	WLC	B.27
“Platão”	DEI	WLC	B.28
“SC06”	OMI	WLC	B.29
“SC06”	DEI	WLC	B.30

OMI

I _N - Agatha - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	100,00%
3	100,00%	100,00%
4	99,47%	99,47%
5	100,00%	100,00%
6	100,00%	100,00%
7	100,00%	100,00%
8	98,40%	98,40%
9	98,94%	98,94%
10	98,40%	97,87%
11	98,40%	98,94%
12	97,87%	97,87%
13	98,40%	98,40%
14	99,47%	98,94%
15	98,40%	98,94%
16	97,87%	97,87%

I _N - Agatha - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%
5	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%
8	98,94%	98,40%	98,40%	98,40%	98,94%	98,94%	98,40%
9	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	98,94%
10	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%
11	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%
12	97,87%	97,87%	97,87%	97,87%	97,87%	98,40%	97,87%
13	98,94%	98,94%	98,94%	98,40%	99,47%	98,94%	98,40%
14	98,40%	98,94%	99,47%	98,94%	99,47%	98,94%	99,47%
15	98,40%	99,47%	99,47%	99,47%	98,40%	99,47%	98,40%
16	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%

I _N - Agatha - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	98,94%	98,94%	98,94%	98,94%	98,94%	98,94%	98,94%	98,40%
9	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%
10	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,94%	97,87%
11	98,40%	99,47%	98,94%	98,94%	99,47%	98,94%	99,47%	98,94%
12	97,34%	98,40%	97,87%	98,40%	98,40%	98,40%	97,87%	98,40%
13	98,94%	98,94%	98,94%	98,94%	98,40%	98,94%	99,47%	99,47%
14	98,94%	98,40%	98,94%	98,40%	98,94%	98,94%	99,47%	99,47%
15	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%
16	97,87%	97,87%	97,87%	96,81%	97,34%	97,87%	97,87%	97,87%

I _N - Agatha - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
2	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	98,94%	98,94%	98,94%	98,94%	98,94%	98,40%	98,94%	98,40%	98,40%
9	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
10	98,94%	98,94%	99,47%	99,47%	97,34%	98,94%	98,94%	98,40%	98,40%
11	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	98,40%	98,40%
12	97,87%	98,40%	98,40%	98,40%	98,40%	98,94%	98,94%	97,87%	97,87%
13	98,94%	99,47%	98,40%	98,94%	99,47%	98,94%	98,40%	98,94%	98,94%
14	97,87%	98,40%	97,87%	97,34%	97,87%	98,94%	97,87%	98,40%	97,34%
15	98,94%	99,47%	99,47%	98,94%	99,47%	98,94%	98,94%	99,47%	98,40%
16	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%	97,87%

I _N - Agatha - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
6	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
9	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%
10	97,87%	98,40%	98,40%	98,94%	98,94%	98,40%	98,94%	98,40%	97,87%
11	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%
12	98,40%	98,94%	98,94%	98,94%	98,94%	98,94%	98,94%	98,94%	98,94%
13	99,47%	98,40%	98,40%	98,94%	98,94%	97,34%	98,40%	99,47%	98,40%
14	98,94%	98,40%	98,94%	97,87%	98,94%	98,40%	98,40%	98,40%	97,87%
15	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%
16	97,87%	97,87%	97,87%	97,87%	97,87%	97,34%	97,87%	97,87%	97,87%

Figura B.7: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Agatha”.

DEI

I _N - Agatha - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	100,00%
3	100,00%	100,00%
4	98,40%	97,87%
5	100,00%	100,00%
6	100,00%	99,47%
7	100,00%	99,47%
8	99,47%	99,47%
9	100,00%	99,47%
10	100,00%	99,47%
11	100,00%	99,47%
12	100,00%	99,47%
13	100,00%	98,40%
14	99,47%	99,47%
15	99,47%	99,47%
16	99,47%	99,47%

I _N - Agatha - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	98,40%	98,40%	98,40%	97,87%	97,87%	97,87%	97,87%
5	99,47%	99,47%	100,00%	100,00%	99,47%	100,00%	98,94%
6	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
9	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
10	100,00%	100,00%	99,47%	98,94%	100,00%	100,00%	99,47%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
12	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	99,47%
13	100,00%	98,94%	100,00%	100,00%	99,47%	99,47%	99,47%
14	99,47%	100,00%	99,47%	99,47%	99,47%	98,94%	99,47%
15	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%
16	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Agatha - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	97,94%
9	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	99,47%	99,47%
10	100,00%	99,47%	100,00%	100,00%	99,47%	99,47%	99,47%	99,47%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
12	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
13	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
14	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
15	100,00%	99,47%	99,47%	100,00%	99,47%	99,47%	100,00%	99,47%
16	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Agatha - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
4	98,40%	98,40%	97,87%	98,40%	97,87%	98,94%	98,40%	98,40%	98,40%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
9	99,47%	100,00%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%
10	100,00%	100,00%	100,00%	100,00%	98,94%	100,00%	98,94%	99,47%	99,47%
11	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%
12	99,47%	100,00%	100,00%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%
13	100,00%	98,94%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%
14	99,47%	100,00%	98,94%	100,00%	99,47%	99,47%	99,47%	99,47%	99,47%
15	99,47%	100,00%	99,47%	100,00%	100,00%	99,47%	99,47%	98,94%	99,47%
16	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Agatha - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	99,47%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	98,94%	98,40%	99,47%	98,94%	98,94%	98,40%	98,40%	99,47%	98,40%
5	99,47%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	100,00%	100,00%
6	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%
7	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%
8	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	98,94%	99,47%
9	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
10	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%
11	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%
13	98,94%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%
14	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%
15	99,47%	99,47%	98,94%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%
16	98,94%	98,94%	99,47%	98,94%	99,47%	98,94%	99,47%	99,47%	99,47%

Figura B.8: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Agatha”.

OMI

I _N - Cana51 - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	100,00%
3	100,00%	100,00%
4	100,00%	100,00%
5	100,00%	100,00%
6	100,00%	100,00%
7	100,00%	100,00%
8	99,47%	99,47%
9	100,00%	100,00%
10	100,00%	100,00%
11	99,47%	99,47%
12	99,47%	99,47%
13	98,40%	98,40%
14	98,94%	98,94%
15	99,47%	99,47%
16	97,87%	97,87%

I _N - Cana51 - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	99,47%	99,47%	99,47%	100,00%	100,00%	100,00%	99,47%
5	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	98,94%
6	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
8	100,00%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
12	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%
13	98,40%	98,40%	98,40%	99,47%	98,94%	98,40%	98,40%
14	98,94%	99,47%	98,94%	98,94%	98,94%	98,94%	98,40%
15	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	97,87%	97,87%	97,87%	98,40%	97,87%	97,87%	97,87%

I _N - Cana51 - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	98,94%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	99,47%
13	98,40%	98,94%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%
14	98,94%	99,47%	99,47%	98,94%	99,47%	100,00%	99,47%	98,94%
15	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	97,87%	98,94%	98,40%	97,87%	97,87%	98,94%	97,87%	98,40%

I _N - Cana51 - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%
4	100,00%	100,00%	99,47%	99,47%	100,00%	99,47%	98,94%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
8	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
12	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	99,47%	99,47%
13	98,40%	98,40%	97,34%	98,40%	98,94%	98,94%	98,40%	98,94%	98,40%
14	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	98,94%
15	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	98,40%	98,94%	98,40%	98,40%	97,87%	98,94%	98,94%	97,87%	97,87%

I _N - Cana51 - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	98,94%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
11	99,47%	99,47%	99,47%	99,47%	100,00%	100,00%	99,47%	98,40%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
13	98,94%	99,47%	98,40%	98,94%	98,40%	98,40%	99,47%	98,40%	98,40%
14	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%
15	99,47%	99,47%	98,40%	98,94%	99,47%	98,94%	99,47%	99,47%	99,47%
16	97,87%	98,94%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	97,87%

Figura B.9: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Cana51”.

DEI

I _N - Cana51 - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	100,00%
3	100,00%	99,47%
4	99,47%	99,47%
5	99,47%	99,47%
6	99,47%	99,47%
7	99,47%	99,47%
8	99,47%	99,47%
9	99,47%	99,47%
10	99,47%	99,47%
11	99,47%	99,47%
12	99,47%	99,47%
13	99,47%	99,47%
14	99,47%	99,47%
15	99,47%	99,47%
16	98,94%	99,47%

I _N - Cana51 - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	99,47%	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%
4	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
5	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
6	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
7	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
8	99,47%	98,94%	98,94%	99,47%	99,47%	99,47%	99,47%
9	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
10	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
11	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	99,47%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
14	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
15	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%

I _N - Cana51 - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%
3	99,47%	99,47%	100,00%	100,00%	99,47%	99,47%	99,47%	99,47%
4	99,47%	99,47%	98,40%	99,47%	99,47%	99,47%	99,47%	99,47%
5	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%
6	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
7	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
8	99,47%	98,94%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%
9	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
10	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
11	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
14	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
15	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Cana51 - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	98,94%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	98,94%	99,47%	99,47%
4	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	98,94%	99,47%
5	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
6	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
7	99,47%	98,40%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
9	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
10	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
11	99,47%	99,47%	99,47%	99,47%	98,94%	98,40%	99,47%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
14	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
15	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	99,47%	98,40%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Cana51 - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
3	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
4	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	99,47%
5	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
6	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%
7	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
9	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
10	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
11	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
14	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%
15	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%

Figura B.10: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Cana51”.

OMI

I _N - Platão - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	99,47%
3	100,00%	100,00%
4	100,00%	99,47%
5	100,00%	100,00%
6	100,00%	100,00%
7	100,00%	100,00%
8	99,47%	98,94%
9	100,00%	100,00%
10	100,00%	100,00%
11	100,00%	100,00%
12	100,00%	99,47%
13	100,00%	99,47%
14	100,00%	99,47%
15	100,00%	99,47%
16	99,47%	99,47%

I _N - Platão - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	99,47%	100,00%	100,00%	99,47%	98,94%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	98,94%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
15	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
16	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%

I _N - Platão - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
8	100,00%	99,47%	99,47%	99,47%	100,00%	100,00%	100,00%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
16	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

I _N - Platão - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	98,94%	98,94%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
11	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
16	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	99,47%

I _N - Platão - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
3	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
4	99,47%	99,47%	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%
5	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
6	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
7	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
8	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	99,47%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	99,47%
13	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%
14	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%
15	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

Figura B.11: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “Platão”.

DEI

I _N - Platão - BGL		
T = 65536		
n	N	
	8	512
1	100,00%	100,00%
2	100,00%	100,00%
3	100,00%	100,00%
4	100,00%	100,00%
5	100,00%	100,00%
6	100,00%	100,00%
7	100,00%	100,00%
8	100,00%	100,00%
9	100,00%	100,00%
10	99,47%	100,00%
11	100,00%	100,00%
12	100,00%	100,00%
13	100,00%	100,00%
14	100,00%	100,00%
15	100,00%	100,00%
16	100,00%	100,00%

I _N - Platão - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	99,47%
6	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
12	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
15	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
16	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - Platão - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%
12	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
13	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
15	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
16	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - Platão - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
4	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
12	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

I _N - Platão - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
11	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
12	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
14	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

Figura B.12: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “Platão”.

OMI

I _N - SC06 - BGL		
T = 65536		
n	N	
	8	512
1	99,47%	100,00%
2	99,47%	100,00%
3	100,00%	100,00%
4	100,00%	100,00%
5	100,00%	100,00%
6	98,94%	99,47%
7	100,00%	99,47%
8	98,40%	98,40%
9	100,00%	99,47%
10	99,47%	99,47%
11	99,47%	98,94%
12	98,40%	97,87%
13	98,40%	97,87%
14	98,94%	98,94%
15	98,40%	97,87%
16	98,94%	98,94%

I _N - SC06 - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
3	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%
4	100,00%	100,00%	100,00%	100,00%	98,94%	100,00%	98,94%
5	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
6	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	98,94%
7	98,94%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	98,40%	98,40%	98,94%	98,94%	98,40%	98,40%	98,40%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
10	98,40%	98,94%	99,47%	99,47%	99,47%	99,47%	98,94%
11	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
12	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	97,87%
13	98,40%	98,94%	98,94%	98,94%	98,94%	98,40%	98,40%
14	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%
15	99,47%	98,94%	98,94%	98,94%	98,94%	98,94%	98,40%
16	99,47%	98,94%	98,94%	98,94%	99,47%	98,94%	98,40%

I _N - SC06 - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
3	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%
4	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	98,94%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
8	98,94%	98,40%	98,40%	98,40%	99,47%	98,40%	98,40%	98,40%
9	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
10	99,47%	99,47%	100,00%	98,94%	99,47%	99,47%	100,00%	98,40%
11	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
12	98,40%	97,34%	98,40%	97,87%	98,94%	97,34%	98,40%	97,87%
13	98,40%	98,40%	98,94%	98,40%	98,94%	98,94%	98,94%	98,94%
14	99,47%	100,00%	99,47%	98,94%	99,47%	100,00%	100,00%	98,94%
15	98,94%	99,47%	98,94%	98,94%	98,94%	98,94%	98,94%	98,40%
16	98,94%	98,94%	99,47%	99,47%	98,94%	98,94%	98,94%	98,40%

I _N - SC06 - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
4	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,40%
5	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	
6	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	100,00%	
7	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	98,94%
8	100,00%	99,47%	99,47%	99,47%	98,40%	99,47%	98,40%	98,40%	
9	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	
10	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	
11	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	100,00%	
12	98,94%	99,47%	98,40%	98,40%	98,94%	99,47%	98,40%	97,87%	
13	99,47%	100,00%	98,94%	100,00%	100,00%	99,47%	98,94%	98,40%	
14	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	98,94%	
15	99,47%	99,47%	100,00%	99,47%	100,00%	100,00%	99,47%	98,40%	
16	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	98,94%	99,47%	98,94%

I _N - SC06 - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
4	98,94%	99,47%	99,47%	100,00%	99,47%	98,94%	99,47%	99,47%	100,00%
5	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
6	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
7	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%
8	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	98,94%	98,40%
9	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	100,00%	99,47%
10	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	99,47%	99,47%
11	98,40%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%	98,94%
12	98,94%	98,94%	98,40%	98,94%	98,40%	98,94%	98,94%	98,94%	98,40%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%
14	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%
15	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	98,94%	99,47%	98,94%
16	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%

Figura B.13: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador OMI processando a fonte “SC06”.

DEI

I _N - SC06 - BGL		
T = 65536		
n	N	
	8	512
1	99,47%	100,00%
2	100,00%	99,47%
3	100,00%	100,00%
4	100,00%	99,47%
5	100,00%	100,00%
6	100,00%	100,00%
7	100,00%	100,00%
8	99,47%	99,47%
9	100,00%	99,47%
10	99,47%	98,40%
11	100,00%	98,94%
12	100,00%	99,47%
13	100,00%	99,47%
14	99,47%	98,94%
15	100,00%	98,94%
16	100,00%	98,94%

I _N - SC06 - BGL							
T = 131072							
n	N						
	8	16	32	64	128	256	1024
1	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%
6	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%
7	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
8	98,94%	99,47%	99,47%	99,47%	99,47%	100,00%	98,94%
9	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%
10	100,00%	100,00%	100,00%	98,94%	98,94%	99,47%	98,94%
11	99,47%	100,00%	100,00%	100,00%	99,47%	99,47%	98,94%
12	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	98,94%
13	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%	99,47%
14	98,94%	99,47%	98,94%	98,94%	99,47%	100,00%	98,40%
15	100,00%	100,00%	99,47%	99,47%	100,00%	99,47%	98,94%
16	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%	98,94%

I _N - SC06 - BGL								
T = 262144								
n	N							
	8	16	32	64	128	256	512	1024
1	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
2	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%
5	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
6	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%
7	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%
8	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%	99,47%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%
10	99,47%	99,47%	98,94%	99,47%	99,47%	100,00%	99,47%	98,94%
11	100,00%	100,00%	100,00%	98,94%	99,47%	99,47%	100,00%	99,47%
12	99,47%	99,47%	100,00%	100,00%	99,47%	99,47%	99,47%	98,94%
13	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	100,00%	99,47%
14	98,94%	100,00%	99,47%	98,94%	99,47%	98,94%	98,94%	99,47%
15	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%
16	100,00%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%	98,94%

I _N - SC06 - BGL									
T = 524288									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%
7	100,00%	99,47%	100,00%	100,00%	98,40%	100,00%	100,00%	100,00%	100,00%
8	100,00%	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%
9	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
10	99,47%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	99,47%	99,47%
11	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	98,94%	100,00%
12	99,47%	99,47%	98,94%	98,94%	99,47%	100,00%	99,47%	98,94%	100,00%
13	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	99,47%
14	100,00%	99,47%	99,47%	100,00%	98,94%	98,94%	99,47%	99,47%	98,94%
15	100,00%	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	98,94%
16	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	99,47%

I _N - SC06 - BGL									
T = 1048576									
n	N								
	8	16	32	64	128	256	512	1024	2048
1	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	99,47%	100,00%	100,00%
4	99,47%	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	100,00%
5	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	100,00%
6	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%
7	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	100,00%
8	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
9	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%
10	98,40%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
11	99,47%	99,47%	99,47%	99,47%	99,47%	98,40%	99,47%	99,47%	99,47%
12	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
13	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
14	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	98,94%	99,47%
15	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%
16	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	99,47%	99,47%	99,47%

Figura B.14: Resultados do Ensaio 2 quando o entrelaçador BGL é empregado no codificador DEI processando a fonte “SC06”.

OMI

I _N - Agatha - WLC										
T = 65536										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	99,47%	100,00%	100,00%	98,94%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
5	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	98,94%	99,47%	99,47%	98,94%	98,94%	98,94%	98,94%	98,94%	99,47%	98,94%
9	98,94%	99,47%	98,94%	99,47%	98,94%	99,47%	98,94%	99,47%	100,00%	99,47%
10	97,34%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
11	99,47%	99,47%	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	98,94%
12	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
13	100,00%	98,94%	99,47%	100,00%	98,94%	99,47%	100,00%	99,47%	99,47%	99,47%
14	99,47%	100,00%	100,00%	99,47%	100,00%	100,00%	98,94%	99,47%	100,00%	99,47%
15	99,47%	100,00%	98,94%	100,00%	98,94%	99,47%	98,94%	99,47%	99,47%	99,47%
16	98,40%	98,40%	98,40%	97,87%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%

I _N - Agatha - WLC										
T = 262144										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	99,47%	98,94%	98,94%	99,47%	98,40%	99,47%	99,47%	99,47%	99,47%
9	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
10	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%
11	99,47%	98,94%	99,47%	99,47%	98,94%	98,94%	99,47%	98,94%	98,94%	98,94%
12	98,94%	98,94%	100,00%	98,94%	98,94%	99,47%	99,47%	98,94%	98,40%	98,40%
13	100,00%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%
14	98,94%	98,94%	98,94%	98,94%	100,00%	98,94%	98,94%	98,94%	98,94%	98,94%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%
16	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%

I _N - Agatha - WLC										
T = 1048576										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
9	99,47%	99,47%	99,47%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	98,94%	98,94%	98,94%	98,40%	99,47%	98,94%	99,47%	98,94%	99,47%	98,40%
11	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	99,47%	100,00%
12	98,94%	100,00%	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	99,47%	99,47%
13	98,94%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
14	99,47%	99,47%	99,47%	99,47%	100,00%	99,47%	100,00%	98,94%	99,47%	98,94%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%

I _N - Agatha - WLC										
T = 131072										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
4	98,94%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%
5	100,00%	98,94%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
8	99,47%	98,94%	98,94%	98,94%	98,94%	98,40%	98,94%	98,40%	98,94%	98,94%
9	100,00%	99,47%	99,47%	100,00%	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%
10	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
11	99,47%	98,94%	99,47%	99,47%	99,47%	98,94%	99,47%	98,94%	99,47%	98,94%
12	98,40%	98,94%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%	98,40%
13	100,00%	100,00%	99,47%	99,47%	99,47%	100,00%	99,47%	99,47%	99,47%	99,47%
14	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%	100,00%	99,47%
15	100,00%	99,47%	100,00%	100,00%	100,00%	99,47%	99,47%	99,47%	100,00%	100,00%
16	97,87%	98,40%	98,40%	98,40%	97,87%	98,40%	98,40%	98,40%	97,87%	98,40%

I _N - Agatha - WLC										
T = 524288										
n	Caso									
	1	2	3	4	5	6	7	8	9	10
1	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
2	100,00%	100,00%	100,00%	100,00%	100,00%	98,94%	100,00%	100,00%	100,00%	99,47%
3	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
4	100,00%	98,40%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%
5	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
6	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
7	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%
8	99,47%	98,94%	98,94%	98,94%	99,47%	98,94%	99,47%	98,94%	99,47%	98,94%
9	100,00%	100,00%	100,00%	99,47%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
10	98,40%	98,94%	98,40%	99,47%	99,47%	98,94%	98,94%	98,94%	98,94%	99,47%
11	99,47%	100,00%	99,47%	99,47%	100,00%	99,47%	100,00%	99,47%	99,47%	100,00%
12	100,00%	100,00%	100,00%	99,47%	100,00%	98,94%	100,00%	99,47%	98,94%	99,47%
13	100,00%	100,00%	100,00%	100,00%	99,47%	99,47%	100,00%	100,00%	100,00%	99,47%
14	98,94%	99,47%	98,94%	99,47%	100,00%	98,94%	99,47%	98,94%	99,47%	98,94%
15	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%
16	98,40%	98,40%	98,40%	98,40%	98,40%	97,87%	97,87%	97,87%	98,40%	98,40%

Figura B.23: Resultados do Ensaio 2 quando o entrelaçador WLC é empregado no codificador OMI processando a fonte “Agatha”.

