



FEDERAL UNIVERSITY OF AMAZONAS

FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING

POSTGRADUATE PROGRAM IN ELECTRICAL ENGINEERING

CHAOS-BASED S-BOXES AS A SOURCE OF CONFUSION IN
CRIPTOGRAPHIC PRIMITIVES

Élvio Carlos Dutra e Silva Júnior

Manaus

June 2026



FEDERAL UNIVERSITY OF AMAZONAS
FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING
POSTGRADUATE PROGRAM IN ELECTRICAL ENGINEERING

CHAOS-BASED S-BOXES AS A SOURCE OF CONFUSION IN
CRYPTOGRAPHIC PRIMITIVES

Élvio Carlos Dutra e Silva Júnior

Doctoral Thesis submitted to the
Postgraduate Program in Electrical
Engineering, PPGEE, of the Faculty of
Electrical and Computer Engineering,
FEEC, of the Federal University of
Amazonas, UFAM, as partial fulfillment of
the requirements to obtain the degree of
Doctor in Electrical Engineering.

Advisor: Carlos Augusto de Moraes Cruz

Manaus

June 2026

Ficha Catalográfica

Elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

S586c Silva Júnior, Élvio Carlos Dutra e
 Chaos-based s-boxes as a source of confusion in cryptographic
 primitives / Élvio Carlos Dutra e Silva Júnior. - 2026.
 203 f. : il., color. ; 31 cm.

 Orientador(a): Carlos Augusto de Moraes Cruz.
 Tese (doutorado) - Universidade Federal do Amazonas, Programa de
 Pós-Graduação em Engenharia Elétrica, Manaus (AM), 2026.

 1. Substitution boxes. 2. Chaos. 3. Chaotic map. 4. Encryption. 5.
 Cryptographic primitives. I. Cruz, Carlos Augusto de Moraes. II.
 Universidade Federal do Amazonas. Programa de Pós-Graduação em
 Engenharia Elétrica. III. Título



Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Programa de Pós-Graduação em Engenharia Elétrica

FOLHA DE APROVAÇÃO

Poder Executivo Ministério da Educação
Universidade Federal do Amazonas
Faculdade de Engenharia Elétrica e Computação
Programa de Pós-graduação em Engenharia Elétrica

Pós-Graduação em Engenharia Elétrica. Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Campus Universitário, Setor Norte - Coroado, Pavilhão do CETELI. Fone/Fax (92) 99271-8954 Ramal:2607. E-mail: ppgee@ufam.edu.br

ÉLVIO CARLOS DUTRA E SILVA JÚNIOR

CHAOS-BASED S-BOXES AS A SOURCE OF CONFUSION IN CRYPTOGRAPHIC PRIMITIVES

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Doutor em Engenharia Elétrica na área de concentração Controle e Automação de Sistemas.

Aprovada em 22 de junho de 2026.

BANCA EXAMINADORA

Prof. Dr. Carlos Augusto de Moraes Cruz - Presidente
Prof. Prof. Dr. Paulo Fernandes da Silva Junior- Membro Titular 1 - Externo
Prof. Prof. Dr. Eduardo Luzeiro Feitosa - Membro Titular 2 - Externo
Profª. Dra Fabíola Guerra Nakamura - Membro Titular 3 - Externo
Prof. Dr. Waldir Sabino da Silva Junior - Membro Titular 4 - Interno

Documento assinado eletronicamente



Documento assinado eletronicamente por **Carlos Augusto de Moraes Cruz, Professor do Magistério Superior**, em 22/06/2026, às 12:38, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Paulo Fernandes da Silva Junior, Usuário Externo**, em 25/06/2026, às 10:16, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Eduardo Luzeiro Feitosa, Professor do Magistério Superior**, em 30/06/2026, às 08:45, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Fabiola Guerra Nakamura, Professor do Magistério Superior**, em 30/06/2026, às 09:26, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Waldir Sabino da Silva Júnior, Professor do Magistério Superior**, em 30/06/2026, às 09:49, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3219131** e o código CRC **D6AA61B1**.

Av. General Rodrigo Octávio Jordão Ramos, nº 3.000 - Bairro Coroado Campus Universitário, Setor Norte
- Telefone: 99271-8954
CEP 69080-900 Manaus/AM - Pavilhão do CETELI. E-mail: ppgee@ufam.edu.br

Referência: Processo nº 23105.022743/2026-13

SEI nº 3219131

*When we do not understand
the intrinsic nature of a
phenomenon,
we portray it in a table.*

*When we reach a complete and
deep knowledge of its behavior,
we represent it in an equation.*

*Prof. Dr. Carl Herrmann Weis
(☆ 1928 † 2013)*

Acknowledgements

“In the beginning, God created the heaven and the earth. . . . And the earth was without form, and void; and darkness was upon the face of the deep. . . . And God said, ‘Let there be light:’ and there was light” (Genesis 1:1–3).

This foundational passage evokes the transition from primordial disorder to intelligible order, a movement that resonates with the very essence of scientific inquiry. From the state described as formless and empty to the emergence of light, structure, and meaning, it reflects the enduring human pursuit of understanding the principles that govern reality, associated with its origin in the chaotic Big Bang.

As a first acknowledgment, I offer my deepest gratitude to God, the Creator of time and space, and of all material and spiritual beings that inhabit them. His infinite wisdom and boundless grace grant us existence and endow us with the capacity to explore, question, and comprehend, even if only partially, the profound complexity and beauty of His creation, from the primordial chaos described as *tohu va-bohu*¹ to the order and beauty that emerge from it. May this work stand as a humble testament to that gift and to the pursuit of understanding it inspires.

God gave us a family. I thank my parents, Élvio Carlos Dutra e Silva and Suzana Frederico Dutra e Silva, for their unwavering support throughout my life; my wife, Sandra Elizabeth Chaves Dutra e Silva, and my daughter, Clara Vitória Dutra e Silva, for their support and understanding during the preparation of this work. I offer them my deepest love and gratitude.

I thank all my ancestors for paving the path that has brought me here. I am grateful to my grandparents, great-grandparents, and all those who came before

¹This Hebrew expression is traditionally translated as “formless and void.” In its original philological context, *tohu* denotes a state of desolation or lack of structure, while *bohu* conveys emptiness or absence of content. Together, the phrase expresses a condition of primordial unformedness, often interpreted in theological and cosmological studies as a pre-ordered state preceding the emergence of structure, order, and intelligibility.

them. I also thank my uncles, my sister, Gláucia Frederico Dutra e Silva, and my cousins. I further extend my gratitude to our descendants—my daughter and nephews—who will carry forward the responsibility of building a better world for future generations.

I would like to express my sincere gratitude to Prof. Dr. Carlos Augusto de Moraes Cruz for accepting me as his advisee, for his patience, and for his invaluable guidance throughout this work. Without his support, this dissertation would not have been possible.

A teacher affects eternity, for no one can tell where their influence ends, shaping minds and futures beyond the limits of time (Adams, 1918). I would like to express my sincere gratitude to all my teachers, professors, instructors, advisors, and mentors, more than 300 professionals who have contributed to my education throughout my life, from elementary education (Escola Madalena Moura Ferro; Colégio Adventista Centro; Instituto Estadual de Educação, in Florianópolis; and Escola Estadual Maria Constança Barros Machado, in Campo Grande), through secondary education (Escola Preparatória de Cadetes do Ar, EPCAr), to higher education (Academia da Força Aérea, AFA; Universidade Federal de Mato Grosso do Sul, UFMS; and Instituto Tecnológico de Aeronáutica, ITA), and postgraduate studies (Escola Superior de Propaganda e Marketing, ESPM; Centro de Estudos em Telecomunicações da PUC-Rio, CETUC; Technische Universität Darmstadt, TUD; Universidade da Força Aérea, UNIFA; Instituto de Controle do Espaço Aéreo, ICEA; Serviço Nacional de Aprendizagem Industrial, SENAI).

I would like to express my special thanks to the institution that hosts this thesis, which admitted me as a student through Notice No. 061/2023 – PROPESP (UFAM), 3 Nov 2023, and to its prominent professors, who have contributed to my academic development: the Federal University of Amazonas (Universidade Federal do Amazonas, UFAM), the Center for Research and Development in Electronic and Information Technology (Centro de Pesquisa e Desenvolvimento em Tecnologia Eletrônica e da Informação, CETELI), and the Graduate Program in Electrical Engineering (Programa de Pós-Graduação em Engenharia Elétrica, PPGE).

Education is not preparation for life but life itself, and it is through experience that knowledge acquires meaning, as practice gives substance and validity to theory

(Dewey, 1897; 1916). In this context, I would like to thank the following institutions and their prominent members for supporting this research in a broad and collaborative context and for contributing to my professional development: the Federation of Industries of the State of Amazonas (FIEAM); the National Directorate (DN) and the Amazonas Regional Directorate (DR-AM) of SENAI, the National Service for Industrial Training; the Superintendency of Innovation and Technology (SITEC); the SENAI Institute of Innovation in Microelectronics (ISI-ME); the Brazilian Society of Microelectronics (SBMicro); Brazilian Association of the Semiconductor Industry (ABISEMI); the Microelectronic Systems (MES) Research Group at Technische Universität Darmstadt (TUD); Rohde & Schwarz GmbH & Co. KG; the University of Leeds (UoL); the Commission for the Coordination and Implementation of the Amazon Surveillance System (SIVAM); the Commission for the Implementation of the Brazilian Airspace Control System (CISCEA); the Integrated Center for Air Defense and Air Traffic Control (CINDACTA I); Operational Coordination Committee for the Rio 2016 Olympic and Paralympic Games; the Institute for Advanced Studies (IEAv); the Commission for Coordination and Implementation of Space Systems (CCISE); Avibras Aerospace Industry; Tecsys Telecommunications Industry; Patria Investments Group; Silver Tiger Consulting (STC).

Resumo da Doctoral apresentada à UFAM como parte dos requisitos necessários para a obtenção do grau de Doctor em Engenharia Elétrica

CAIXAS DE SUBSTITUIÇÃO (S-BOXES) BASEADAS EM CAOS COMO FONTE DE CONFUSÃO EM PRIMITIVAS CRIPTOGRÁFICAS

Élvio Carlos Dutra e Silva Júnior

Advisor: Carlos Augusto de Moraes Cruz

Programa: Postgraduate Program in Electrical Engineering

O presente trabalho apresenta duas contribuições principais. A primeira consiste em uma Revisão Sistemática da Literatura (RSL) sobre criptografia baseada em caos, com foco em caixas de substituição (S-boxes) como primitivas criptográficas, sendo, até onde se pôde verificar, a primeira RSL dessa natureza, conforme evidenciado por meio de um levantamento de revisões da literatura (SoS – *Survey of Surveys*). A segunda contribuição, identificada como original a partir da RSL inédita conduzida nesta tese, refere-se à implementação de uma Caixa de Substituição Baseada em Caos (CB-SBox), na qual S-boxes convencionais baseadas em ROM são substituídas por um circuito digital que computa diretamente um mapa caótico devidamente selecionado.

Nos últimos anos, diversos algoritmos de criptografia baseados em caos têm sido propostos. Muitos desses algoritmos baseiam-se em projetos já estabelecidos e preenchem suas S-boxes (caixas de substituição) com valores derivados de mapas caóticos, seguindo estratégias convencionais de implementação a fim de possibilitar a comparação com seus equivalentes não caóticos.

Em contraste, este trabalho propõe uma abordagem inovadora: a implementação de uma Caixa de Substituição Baseada em Caos (CB-SBox), na qual S-boxes convencionais baseadas em ROM são substituídas por um circuito digital que computa diretamente um mapa caótico devidamente selecionado. Este método permite a construção de S-boxes com grandes tamanhos de palavra por meio de um circuito

programável baseado em FPGA, possibilitando o uso de tamanhos configuráveis de S-boxes, o que facilita a análise de estruturas com diferentes dimensões e, em última instância, pode aumentar a segurança, particularmente para S-boxes de maior dimensão, conforme evidenciado pelo aumento da resistência à criptoanálise linear e diferencial.

Além disso, a CB-SBox proposta apresenta reduções tanto na área quanto no consumo de energia em comparação com S-boxes convencionais baseadas em ROM e de tamanho equivalente. Uma S-box de 19 bits baseada em caos consome apenas 0.0238% da área e 0.0241% da energia exigidas por uma S-box equivalente implementada em ROM, mantendo o mesmo nível de segurança.

A imprevisibilidade inerente ao comportamento caótico não linear faz com que as S-boxes propostas apresentem características não bijetivas, tornando-as adequadas para aplicação em primitivas criptográficas não invertíveis, como funções de hash e redes de Feistel. A CB-SBox proposta é implementada em uma rede de Feistel conforme descrito na literatura, e os resultados experimentais são apresentados.

Palavras-chave: caixas de substituição (S-boxes); caos; mapa caótico; criptografia; primitivas criptográficas; redes de Feistel; análise criptográfica linear e diferencial; matriz de portas lógicas programáveis em campo (FPGA); circuito programável baseado em FPGA; circuito integrado de aplicação específica (ASIC) .

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

CHAOS-BASED S-BOXES AS A SOURCE OF CONFUSION IN CRYPTOGRAPHIC PRIMITIVES

Élvio Carlos Dutra e Silva Júnior

Advisor: Carlos Augusto de Moraes Cruz

Department: Postgraduate in Electrical Engineering

This work presents two main contributions. The first consists of a Systematic Literature Review (SLR) on chaos-based cryptography, with a focus on substitution boxes (S-boxes) as cryptographic primitives. To the best of the authors' knowledge, this is the first SLR of this nature, as evidenced by a survey of literature reviews (SoS – *Survey of Surveys*). The second contribution, original as identified on the novel SLR conducted in this work, concerns the implementation of a Chaos-Based Substitution Box (CB-SBox), in which conventional ROM-based S-boxes are replaced by a digital circuit that directly computes a suitably selected chaotic map.

In recent years, numerous chaos-based encryption algorithms have been proposed. Many of these approaches build upon established encryption designs and populate their S-boxes with values derived from chaotic maps, following conventional implementation strategies to enable comparison with their non-chaotic counterparts.

In contrast, this work proposes a novel approach: a Chaos-Based Substitution Box (CB-SBox) implementation, in which conventional ROM-based S-boxes are replaced by a digital circuit that directly computes the next state of a suitably selected chaotic map. This method enables the construction of S-boxes with large word lengths through an FPGA-based programmable circuit that supports configurable S-box sizes, thereby facilitating the analysis of structures with varying dimensions and, ultimately, enhancing security, particularly for larger S-boxes, as evidenced by increased resistance to linear and differential cryptanalysis.

Furthermore, the proposed CB-SBox achieves reductions in both area and power consumption compared to size-equivalent ROM-based S-boxes. A 19-bit chaos-based S-box consumes only 0.0238% of the area and 0.0241% of the power required by an equivalent ROM-based S-box, while maintaining the same level of security.

The inherent unpredictability of nonlinear chaotic behavior leads the proposed chaos-based S-boxes to exhibit non-bijective characteristics, making them well suited for application in non-invertible cryptographic primitives, such as hash functions and Feistel networks. The proposed CB-SBox is implemented within a Feistel network, as described in the literature, and experimental results are presented.

Keywords: substitution boxes (s-boxes); chaos; chaotic map; encryption; cryptographic primitives; Feistel networks; linear and differential cryptanalysis; field-programmable gate array (FPGA); FPGA-based programmable circuit; application-specific integrated circuit (ASIC).

Contents

1	Introduction	1
1.1	Contextualization	1
1.2	Research Problem and Hypotheses	2
1.3	Motivation and Justification	3
1.4	Overall and Specific Objectives	4
1.5	Scientific Contributions	5
1.6	Scope Definition	6
1.6.1	Beyond the Scope	7
1.7	Chapter Organization	9
2	Theoretical Framework	12
2.1	Cryptography Principles	12
2.1.1	Cryptographic Building Blocks	13
2.1.2	Cryptanalysis and Security Evaluation	16
2.1.3	Cryptographic Systems and Applications	17
2.2	Chaos Theory	18
2.2.1	Scientific Principles	19
2.2.2	Chaos Properties	22
2.2.3	Chaotic Systems	28
3	State-of-the-Art	37
3.1	Chapter Introduction	37
3.2	Survey of Surveys: Literature Positioning	38
3.2.1	Methodology	39
3.2.2	Data Extraction	41

3.2.3	Synthesis and Analysis	55
3.3	Systematic Literature Review: New Frontiers	57
3.3.1	Methodology	60
3.3.2	Data Extration	63
3.3.3	Synthesis and Analysis	98
3.4	Chapter Conclusions	130
4	Materials and Methods	132
4.1	Materials	132
4.2	Methods	135
5	Experimental Results	139
5.1	Chapter Introduction - CB-SBox	139
5.2	Chaotic Map Evaluation	140
5.3	Chaos-Based Substitution Box (CB-SBox)	145
5.4	CB-SBox Performance Analysis	148
5.4.1	Area and Power Analysis	149
5.4.2	Timing Analysis	151
5.4.3	Security Analysis	156
5.4.4	Bijectivity Analysis	156
5.4.5	Joint Analysis	159
5.5	CB-SBox in a Feistel Network	160
5.6	Chapter Conclusions - CB-SBox	168
6	Conclusions	171
6.1	Timeline	171
6.2	Contributions of This Thesis	173
6.3	Future Work	180
	Bibliography	182

List of Figures

1.1	Graphical Abstract	2
1.2	Hierarchical representation of the scope definition adopted in this thesis.	8
2.1	Visualization of the Mandelbrot set, a well-known fractal illustrating chaotic behavior in dynamical systems. Source: HypeScience, accessed May 30, 2025.	19
3.1	PRISMA diagram of study selection in the SoS	42
3.2	PRISMA diagram of study selection in the SLR	84
3.3	Distribution of publication sources in the initial study pool	99
3.4	Distribution of application domains in the initial study pool	99
3.5	Temporal distribution of publications in the initial study pool	100
3.6	Temporal distribution of publications in the included studies	105
3.7	Geographical distribution of publications in the included studies	106
3.8	Distribution of publications across publishers in the included studies	107
3.9	Distribution of application domains in the included studies	108
4.1	Software package	133
4.2	Xilinx Spartan-3 development board	134
4.3	Power and data cables used in a Xilinx Spartan-3 development setup	135
4.4	Experimental setup used for the design, simulation, and validation of the proposed solution.	137
4.5	Methodological workflow adopted in the research.	138
5.1	Three-dimensional V_{IC} , computed for the Sprott B chaotic map [1], adapted from [2], and made available online in [3] to support three-dimensional visualization.	142

5.2	Schematic circuit view of the CB-SBox model and its Sprott B subsystem, available in [3]. (a) CB-SBox. (b) Sprott B [1] subsystem of Equation (5.7).	147
5.3	Area comparison between ROM-Based and CB-SBox implementations as a function of circuit input size (NOB).	150
5.4	Power consumption comparison between ROM-Based and CB-SBox implementations as a function of circuit input size (NOB).	150
5.5	Time response of the CB-SBox: LongRun parameter required to decorrelate outputs from inputs, as a function of the circuit size measured in NOB.	152
5.6	Visualization of a cube with 729 ICs (in green) and the three-dimensional dispersion of their corresponding final states (in blue) over the Sprott B attractor $\mathcal{A}$ (in yellow), available online in [3].	153
5.7	Visualization of a grid of <i>Initial Conditions</i> (ICs) (blue) and the corresponding final state dispersion (red), generated by trajectories evolving on the Sprott B chaotic attractor $\mathcal{A}$ in a dimensionless state space. The results are presented as a 2D projection of the 3D phase space. The dataset is available online in [3].	154
5.8	Spatial distribution of LongRun parameter (within the graph) for 79 groups of 500 ICs in the plane $z = -17.0625$, with $DC = 30$	155
5.9	Security analysis based on the computation time (seconds) in y-axis required to evaluate the Linear and Differential Probability Biases of S-Boxes as a function of their size (NOB) in x-axis, available online in [3].	157
5.10	Schematic diagram of the encryption block cipher, where the CB-SBox, embedded within each f_k subsystem and previously detailed in Figure 5.2, is highlighted in blue.	161
5.11	Schematic representation of the decryption block cipher.	162
5.12	FPGA performance of the block cipher.	163
5.13	Results of applying the 152-bit recursive block cipher to the ‘Lena’ image.	165

5.14	Original and encrypted versions of the LaTeX text, encrypted using the 152-bit recursive block cipher based on the CB-SBox.	166
5.15	Histograms after applying the 152-bit encryption process, which em- ploys the proposed CB-SBox, to the abstract of this paper, written in LaTeX. The corresponding dataset is available online [3].	167

List of Tables

3.1	Selected literature reviews in the SoS	51
3.2	Positioning of this SLR within chaos-based cryptography surveys . . .	59
3.3	Selected primary studies for the SLR	85
3.4	S-Box evaluation metrics identified in the reviewed studies	116
3.5	Cipher evaluation metrics identified in the reviewed studies	117
5.1	Performance comparison of six selected chaotic maps according to the four-parameter evaluation method proposed in [4], available online in [3].	144
5.2	The dimensions of three non-overlapping parallelepipeds belonging to the V_{IC} shown in Figure 5.1, available online in [3].	148
5.3	Statistical analysis of the bijectivity of CB-SBoxes, where NOB de- notes the number of bits, followed by the corresponding table length that equals 2^{NOB} and the calculated bijectivity index (data available online in [3]).	158
6.1	Schedule of Activities	174
6.2	Summary of Selected Stand-Alone Literature Reviews on Chaos-Based Cryptography	175
6.3	Systematic Review Table for Topics: Chaos, Encryption, and <i>Substitution- Boxes</i> (S-Boxes)	176

Acronyms

V_{IC} *Volume of Valid Initial Conditions* 145, 146, 148, 149, 151, 152, 157, 162, 173, 174

V_{Sub} *Largest Subset Volume* 145, 146, 148, 149

χ^2 *Chi-Square Variance* 9, 81, 83, 92–94, 96, 98, 117, 119, 183–186

A *Strange Attractor* 145, 147–150, 157, 162

d_A *Attractor Density* 145, 148, 149

ds *Small Distance* 147, 148

1D-LTS *1-D Logistic Tent chaotic System* 82

1D-STs *1-D Sine-Tent piecewise chaotic System* 80, 81

2D-LSCM *2-D Logistic-Sine-Coupling chaotic Map* 80, 81

ACM *Association for Computing Machinery* 41, 42, 100, 101

AES *Advanced Encryption Standard* 10, 102, 103, 106, 124

AI *Artificial Intelligence* 48, 105, 186

ASIC *Application-Specific Integrated Circuit* 116, 120, 132, 144, 153, 174

AvgDecT *Average Decryption Time* 76

AvgEncT *Average Encryption Time* 76

AvgEncTh *Average Encryption Throughput* 76

AvgNCPB *Average Number of CPU Cycles per Byte* 76

BASE *Bielefeld Academic Search Engine* 41

BFA *Brute-Force Attacks* 9, 18, 19, 45, 76, 77, 92, 118, 184, 186

BIC *Bit Independence Criterion* 9, 17, 70–72, 77, 78, 82, 89, 94, 96, 117, 118, 123, 184, 186

BIC-NL *BIC considering nonlinearity* 9, 74, 96, 184, 186

BIC-SAC *BIC considering the Strict Avalanche Criterion* 9, 74, 92, 96, 184, 186

BRAM *Block Random-Access Memory* 78

CB-SBox *Chaos-Based Substitution-Box* 5–7, 9–11, 136, 138, 143, 144, 150–153, 155, 156, 159–169, 171, 173–175, 180, 186, 187

CBC *Cipher Block Chaining* 15

CCA *Chosen-Ciphertext Attacks* 9, 18, 83, 84, 92, 117, 119, 121, 184, 186

CFI *Choquet Fuzzy Integral* 84

CML *Coupled-Map Lattice* 50

CORE *COnnecting REpositories* 41

CPA *Chosen-Plaintext Attacks* 9, 18, 72, 76, 80, 83, 84, 92, 94, 117, 119, 121, 184–186

CPU *Central Processing Unit* 135

CSK *Chaos Shift Keying* 46

CTR *Counter Mode* 15

CVES *Chaotic Video Encryption Scheme* 69

DAP *Differential Approximation Probability* 4, 9, 70, 74, 77, 78, 82, 89, 92, 94, 96, 117, 118, 180, 184, 185

DC *Discretization Criterion* 151, 152, 156, 157, 159

DCSK *Differential Chaos Shift Keying* 45, 46

DCT *Discrete Cosine Transform* 46, 49, 51

DDR *Double Data Rate* 136, 139

DES *Data Encryption Standard* 10, 15, 102

DFT *Discrete Fourier Transform* 51

DICOM *Digital Imaging and Communications in Medicine* 104

DNA *Deoxyribo Nucleic Acid* 9, 46–50, 58, 75, 76, 84, 103, 105, 112, 113, 115, 122, 186

DSA *Digital Signature Algorithm* 16

DTLS *Datagram Transport Layer Security* 17

DTR *Distance to Time Ratio* 146–149

DWT *Discrete Wavelet Transform* 46, 49, 51

ECB *Electronic Codebook* 15

ECC *Elliptic Curve Cryptography* 49, 50, 58, 92, 94, 115, 184, 185

ECDSA *Elliptic Curve Digital Signature Algorithm* 16, 58

EQlty *Encryption Quality* 76

Fiat-Shamir *Fiat-Shamir Transformation* 16

FPGA *Field-Programmable Gate Array* 7, 45, 51, 65, 78, 102, 103, 109, 115, 116, 120, 123, 132, 136, 138, 143, 153, 167, 169, 171

FrFT *Fractional Fourier Transform* 51

FSM *Finite State Machine* 78, 113

FSR *Feedback Shift Register* 14, 15

GFN *Generalized Feistel Network* 15

GLCM *Gray Level Co-occurrence Matrix* 76, 80, 83, 95, 118, 183

GNCML *Global Nonlocal Collapsible Mapping Lattice* 50

HMAC *Hash-based Message Authentication Code* 16

IC *Initial Condition* xvi, 6, 39, 66, 70, 111–113, 143, 145–149, 151, 157, 159, 162, 167, 173, 174, 187

IEEE *Institute of Electrical and Electronics Engineers* 41, 42, 45, 47, 100, 101, 108, 178, 210

IoT *Internet of Things* 14, 15, 17, 48, 49, 104, 110, 178

IS *Information Systems* 40

ISDNCML *Improved Sinusoidal Dynamic Non-Adjacent Coupled-Map Lattice* 51

ISI-ME *SENAI Institute of Innovation in Microelectronics - Instituto SENAI de Inovação em Microeletrônica* 177

ITA *Aeronautics Institute of Technology - Instituto Tecnológico de Aeronáutica* 4

Jisc *Joint Information Systems Committee* 41

KAM *Kolmogorov-Arnold-Moser* 23, 24

KPA *Known-Plaintext Attacks* 9, 18, 45, 76, 94, 121, 185, 186

LAP *Linear Approximation Probability* 4, 9, 74, 77, 78, 82, 89, 92, 94, 96, 117, 118, 180, 184

LCD *Liquid Crystal Display* 136, 139

LFSR *Linear Feedback Shift Register* 14, 15, 45, 78, 113

LongRun *Long Running Time* 152, 156–159, 162, 167, 173, 174, 187

LUT *Look-Up Table* 6, 78, 113, 123, 143

MAC *Message Authentication Codes* 16

MAE *Mean Absolute Error* 76, 118

MATLAB *MATrix LABoratory* 51, 76, 80, 81, 115, 116, 120, 123, 135, 138

MAZa *Malik, Atif, and Zahid chaotic Map [5]* 77

MD5 *Message Digest Algorithm 5* 16

MDC *Modification Detection Codes* 16

MDCML *Multiple Dynamic Coupled-Map Lattice* 50

MDPI *Multidisciplinary Digital Publishing Institute* 41, 42, 100, 101, 108, 177, 178

MDT *Maximum Dispersion Time* 147–149

MELP *Maximum Expected Linear Probability* 89, 184

MLC *Majority Logic Criteria (statistical tests)* 9, 75, 90, 93, 96, 118, 182, 184, 186

MSE *Mean Square Error* 49, 50, 80, 94, 96, 117–119, 184

NCMLP *Non-Adjacent Coupled Dynamic Parameter Mapping Lattice* 51

NIST *National Institute of Standards and Technology* 9, 17, 69, 76, 79, 83, 89, 93, 95, 117, 119, 124, 131, 183, 184, 186

NL *Nonlinearity* 9, 33, 65, 67, 70–74, 77, 78, 82, 89, 92, 94, 96, 117, 118, 131, 132, 184–186

NLFSR *Nonlinear Feedback Shift Register* 14

NOB *Number of Bits* 151–153, 155, 156, 160–164, 167, 173, 174, 187

NoR *Not a Review* 58

NPCR *Number of Pixel Change Rate* 9, 46–51, 72, 73, 76, 79, 81–83, 92, 94, 96, 117, 119, 131, 184–186

OCML *One-Way Coupled-Map Lattice* 50

OLED *Organic Light-Emitting Diode* 136, 139

OtF *On-the-Fly* 6, 7, 62, 85, 111, 123, 126, 143, 144, 164, 173, 180

P-Box *Permutation-Box* 82

P-Boxes *Permutation-Boxes* 15, 39, 82

PhD *Doctor of Philosophy* 11, 176–179, 186

PICOC *Population, Intervention, Comparison, Outcome and Context* 41, 42, 62, 127, 128

PPGEE *Graduate Program in Electrical Engineering - Programa de Pós-Graduação em Engenharia Elétrica* 12, 176–178

PRISMA *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* 43, 49, 59, 65

PRM *Parallelepiped Relations Measurements* 151, 152, 156, 165, 173

PRNG *Pseudorandom Number Generator* 45, 69, 72, 92, 94, 115, 184, 185

PSNR *Peak Signal-to-Noise Ratio* 9, 49, 50, 76, 80, 94, 96, 117, 119, 184, 186

PWLCM *Piecewise Linear Chaotic Map* 96, 184

R&D *Research and Development* 177

RAM *Random Access Memory* 72, 135

RFID *Radio Frequency Identification* 15

RGB *Red-Green-Blue* 75, 76

ROM *Read Only Memory* 153, 155, 156, 159, 161, 163, 164, 167–169, 171, 173, 175

RSA *Rivest–Shamir–Adleman* 16, 17, 49, 58

S-Box *Substitution-Box* 4–7, 9, 40, 42, 44, 46, 53, 56, 59, 61, 63, 64, 69–78, 80–84, 87–94, 96–100, 102–106, 110, 111, 113, 115–118, 124–126, 131, 137, 143, 144, 159, 160, 163, 164, 167, 171, 174, 175, 180–185, 187, 210

S-Boxes *Substitution-Boxes* xviii, 3, 6, 7, 9, 11, 15, 39, 40, 44, 47, 59, 60, 62, 69–71, 73–80, 82–84, 87, 88, 90, 92, 95, 103, 109–111, 113–115, 117, 119, 120, 123–126, 128–133, 137, 142, 143, 150, 153, 156, 160–164, 168, 171, 173–175, 180, 182, 183, 210

SAC *Strict Avalanche Criterion* 9, 70–72, 74, 77, 78, 82, 89, 92, 94, 96, 117, 118, 123, 184, 186

SCA *Side-Channel Attacks* 15, 16, 18

SDRAM *Synchronous Dynamic Random-Access Memory* 136, 139

SENAI *Brazilian National Industrial Training Service - Serviço Nacional de Aprendizagem Industrial* 177

SHA *Secure Hash Algorithm* 16, 75, 76

SIPI *Signal and Image Processing Institute* 81

SLR *Systematic Literature Review* 6, 7, 11, 40–42, 49, 50, 56, 58–62, 64, 69, 100, 105, 106, 108–112, 119, 120, 122, 124–133, 137, 179–181, 186, 210

SMS *Systematic Mapping Study* 56, 58, 61, 181

SoC *System-on-a-Chip* 89, 109, 115, 116, 123, 184

SoS *Survey of Surveys* 6, 7, 11, 40–42, 59, 125, 127, 128, 132, 137, 186, 210

SOTA *State-of-the-Art* 7, 11, 40, 42, 45, 48, 50, 56, 58, 61, 100, 111, 115, 122, 123, 125, 126, 132, 181

SP800-22 *Special Publication 800-22* 9, 17, 69, 76, 79, 186

SPN *Substitution-Permutation Network* 9, 15, 82, 94, 111, 115, 184

SRAM *Static Random-Access Memory* 136, 139

SSIM *Structural Similarity Index Measure* 50, 80

UACI *Unified Average Changed Intensity* 9, 46–51, 72, 73, 76, 80–83, 92, 94, 96, 117, 119, 131, 184–186

UAV *Unmanned Aerial Vehicle* 51, 52

UFAM *Federal University of Amazonas - Universidade Federal do Amazonas* 12,
176–178

USC *University of Southern California* 81

UWB *Ultra-Wide Band* 45

VHDL *VHSIC Hardware Description Language* 144, 153

WoS *Web of Science* 41, 42, 47

Chapter 1

Introduction

Framing the Research Problem and Outlining the Path Forward

1.1 Contextualization

Since Lorenz's 1963 seminal article [6], more than forty non-linear differential equations presenting chaotic behavior have been reported [1, 7–13]. They have been applied to many disciplines, such as mechanics [14], biology [15], ecology [16], astronomy [17], and cryptography [5, 18–61].

Chaos and encryption are intimately tied: confusion (typically achieved through nonlinear substitutions in the encryption process to obscure the relationship between the ciphertext and the encryption key) and diffusion (generally implemented through permutation and mixing operations to ensure that the influence of a single plaintext bit spreads over many ciphertext bits), two fundamental concepts of cryptography [62], are closely associated with the chaotic properties of ergodicity and sensitivity to initial conditions [63]. Sensitivity to initial conditions ensures that even minimal changes in the input, such as slight variations in the secret key, produce significantly different outputs, thereby enhancing key sensitivity and resistance to differential attacks. Ergodicity allows chaotic maps to eventually cover the entire state space, contributing to the statistical uniformity of encrypted outputs and enhancing resilience against cryptanalysis. Although deterministic, chaotic maps exhibit highly complex dynamics, resulting in outputs that appear random

while providing a desirable balance between reproducibility and unpredictability. This complexity reinforces confusion, while the topological mixing property of chaos facilitates effective diffusion, ensuring that small changes in the plaintext or key propagate throughout the ciphertext. These features make chaos an attractive and powerful foundation for the design of robust cryptographic systems.

This work lies in the domain of applying chaos theory as a source of randomness for cryptographic algorithms, as graphically illustrated on Figure 1.1.



Figure 1.1: Graphical Abstract

1.2 Research Problem and Hypotheses

This research investigates the applicability of chaos theory to the design of cryptographic mechanisms that achieve strong security properties. In particular, this work aims to develop and evaluate an encryption algorithm that leverages chaotic maps derived directly from nonlinear differential equations governing chaotic systems. Instead of relying on precomputed values, the proposed approach numerically integrates continuous-time chaotic dynamics with finite precision and embeds them as a core component of the encryption process. The study focuses on incorporat-

ing key chaotic features—such as ergodicity, sensitivity to initial conditions, and complex mixing—into the construction of the cipher.

The research problem can therefore be stated as follows: Can the intrinsic dynamics of chaotic systems, expressed through nonlinear differential equations, be reliably and securely applied to construct robust cryptographic primitives for message encryption?

Building on the research problem presented, this study proposes the following hypotheses, which serve as testable propositions guiding the development and evaluation of the cryptographic mechanisms:

- **H1:** Continuous-time chaotic dynamics, derived from nonlinear differential equations, can be digitally integrated with sufficient precision to produce the output values of robust S-Boxes, exploiting chaotic properties to enhance cryptographic security.
- **H2:** Encryption algorithms based on continuous-time chaotic dynamics can achieve strong cryptographic properties, as measured by *Differential Approximation Probability* (DAP) and *Linear Approximation Probability* (LAP), with performance comparable to or exceeding that of conventional *Substitution-Box* (S-Box) designs.
- **H3:** Chaos-based cryptographic primitives can be efficiently implemented in hardware platforms (e.g., FPGA), achieving scalability and competitive performance for sufficiently large S-Box sizes.

1.3 Motivation and Justification

One of the central motivations for this research lies in the inherent parallel between cryptography and the act of shuffling a deck of cards. In cryptographic terms, encrypting a message is analogous to scrambling a sequence of data using a deterministic and reversible process, just as one might shuffle a deck in a way that, given the exact method and order of operations, allows it to be perfectly unshuffled. Traditional chaos-based cryptographic schemes often rely on generating pseudoran-

dom sequences from iterated chaotic maps to drive this scrambling, treating chaos as a source of entropy or key streams [21, 25, 26, 37, 38].

This research proposes a more direct and potentially superior alternative. Instead of relying on offline precomputed outputs of chaotic systems, it aims to employ the underlying nonlinear differential equations themselves as the core encryption mechanism. By embedding the continuous-time dynamics of chaotic systems into the encryption process in finite-precision digital form, the algorithm can more effectively exploit key chaotic properties. These characteristics naturally reinforce the cryptographic principles of confusion and diffusion, as outlined by Shannon [62], and echo a profound insight from the late Prof. Carl Hermann Weis, former professor at *Aeronautics Institute of Technology - Instituto Tecnológico de Aeronáutica* (ITA)¹: “*When we do not understand the intrinsic nature of a phenomenon, we portray it in a table. When we reach a complete and deep understanding of its behavior, we represent it in an equation.*” This perspective underscores the motivation to base cryptographic design directly on the fundamental equations governing chaotic behavior.

1.4 Overall and Specific Objectives

The overall objective of this research is to design, implement, and evaluate a cryptographic algorithm that employs the intrinsic dynamics of chaotic systems, governed by nonlinear differential equations, as the foundation for secure message encryption. The algorithm aims to directly integrate the continuous-time behavior of physical chaotic systems, numerically computed under finite-precision constraints, in order to preserve essential chaotic properties within the encryption scheme. Through this approach, the research seeks to investigate the feasibility and effectiveness of

¹Carl Hermann Weis (☆ 1928 † 2013) was born in Germany and taught chemistry at ITA from 1952 until the late 1990s, when he was compulsorily retired upon reaching the mandatory retirement age. Professor Weis was also a researcher, having earned his Master’s and Ph.D. degrees in Chemistry from Louisiana State University, Baton Rouge (LA, USA). His academic and educational achievements established Weis as one of the most prominent chemistry researchers to have worked in Brazil. His commitment and dedication to students, his passion for teaching, and his involvement in fostering excellence in education made Weis an undeniable role model for educators. The Weis Award (In Recognition of Excellence in Teaching) celebrates the importance of teachers’ dedication, honoring those like Carl Hermann Weis who have left and continue to leave a lasting inspirational legacy.

using chaos as a robust and secure foundation for constructing cryptographic primitives.

To achieve the overall objective, this research defines the following specific objectives:

- To study and select a suitable chaotic system governed by nonlinear differential equations with desirable characteristics for cryptographic applications.
- To develop a numerical integration scheme capable of simulating the continuous-time dynamics of chaotic systems under finite-precision constraints.
- To design a S-Box, referred to as *Chaos-Based Substitution-Box* (CB-SBox), based on the selected chaotic system for on-the-fly output computation.
- To design a cryptographic algorithm that incorporates the proposed CB-SBox into the confusion component.
- To implement the proposed algorithm in a digital platform and evaluate its performance, including throughput and resistance to cryptographic attacks.
- To compare the proposed method with conventional encryption techniques in terms of security, statistical randomness, and computational cost.

1.5 Scientific Contributions

This work presents two main and original contributions, which are detailed in Chapters 3 and 5.

The first contribution is an original *Systematic Literature Review* (SLR), discussed in Chapter 3. Initially, we conducted a *Survey of Surveys* (SoS) and examined surveys and reviews on chaos-based cryptography. This SoS identified several research gaps, including the absence of systematically constructed literature reviews (SLR) focused on mapping primary studies on chaos-based cryptography that employ S-Boxes as cryptographic primitives. Therefore, this contribution consists of an original SLR addressing the application of chaos theory to the design of S-Boxes for cryptographic systems.

The second contribution is a novel CB-SBox, presented in Chapter 5. The conducted SLR (Chapter 3) identified several research gaps, among them the absence of an S-Box implementation in which traditional *Look-Up Table* (LUT) structures, such as those presented in [5, 21, 23, 24, 26–29, 32–39, 41, 43–45, 47, 48, 50–53, 56, 57], are replaced by an on-the-fly fixed-point arithmetic computation of a nonlinear chaotic differential equation. This structure is referred to as a CB-SBox and offers notable advantages in terms of area, power consumption, and cryptographic strength. Its temporal evolution drives the initial state x_0 , also referred to as the IC, toward a deterministically related yet uncorrelated final state x_f . The final state is reached after executing the chaotic map for a fixed number of iterations. To the best of the authors’ knowledge, this is the first attempt to design a chaotic S-Box based on this *On-the-Fly* (OtF) approach.

1.6 Scope Definition

This thesis focuses on the design, implementation, and evaluation of chaos-based substitution boxes for cryptographic applications, with particular emphasis on a novel programmable CB-SBox architecture. The scope encompasses both a systematic investigation of the *State-of-the-Art* (SOTA) and the development of an *Field-Programmable Gate Array* (FPGA)-based hardware solution grounded in nonlinear chaotic dynamics.

From a methodological perspective, the study is restricted to the application of chaos theory to cryptographic primitives, specifically addressing the construction of S-Boxes through the hardware realization of nonlinear chaotic differential equations. In this approach, continuous-time chaotic systems are discretized and implemented on FPGA platforms using fixed-point arithmetic. The literature analysis is limited to works that explicitly employ chaos-based mechanisms for S-Box design.

Additionally, the scope includes a structured study composed of a SoS followed by a systematic literature review (SLR). The SoS is used to identify, classify, and analyze existing surveys on chaos-based cryptography, providing a high-level understanding of the field and revealing research gaps. Based on these findings, the

SLR focuses on mapping and analyzing primary studies that address the design of chaos-based S-Boxes, ensuring methodological rigor, reproducibility, and comprehensive coverage of the relevant literature.

From an implementation standpoint, the proposed solution targets digital hardware platforms, with emphasis on multi-rate FPGA-based architectures in which values are computed OtF. The evaluation considers metrics such as area utilization, power consumption, as well as standard cryptographic security criteria, including resistance to linear and differential cryptanalysis.

1.6.1 Beyond the Scope

This work does not address the design of complete cryptographic protocols or full encryption systems beyond the integration context required to validate the proposed S-Box. In addition, conventional algebraic or purely heuristic approaches not grounded in nonlinear dynamical systems theory are excluded. Analog implementations, quantum cryptographic approaches, and non-chaotic S-Box constructions are also considered outside the scope of this thesis.

A large number of chaotic systems and maps have been reported in the literature [1, 7–13]. This work focuses on the evaluation of six representative chaotic systems. The investigation of additional chaotic systems and maps, including higher-order systems and superchaotic systems, is beyond the scope of this study and is suggested as future work.

Although chaos theory has broad applications in cryptography, this thesis focuses on the use of chaos in S-Boxes within Feistel networks. Other applications, such as hash functions and asymmetric ciphers, are not addressed and are left for future investigation. Furthermore, extensions involving hybrid approaches, including *Deoxyribo Nucleic Acid* (DNA)-based techniques, quantum computing, and *Substitution-Permutation Network* (SPN) architectures, are beyond the scope of this work.

While several metrics and methodologies exist for analyzing S-Boxes and Feistel networks, this study does not aim to provide an exhaustive evaluation across all available criteria or to propose a unified evaluation framework. A comprehensive assessment using extended metrics, such as *Nonlinearity* (NL), *Chi-Square Variance*

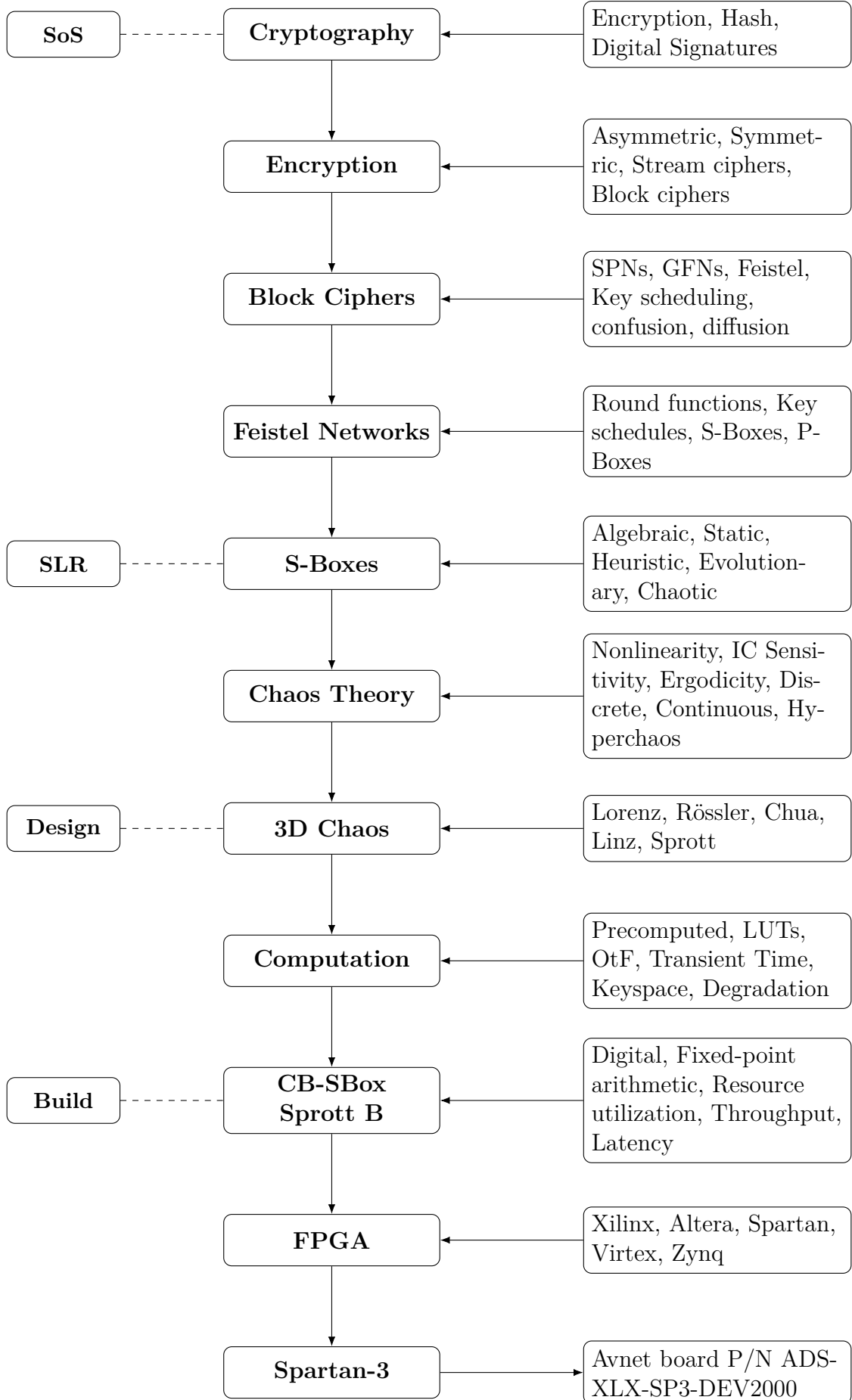


Figure 1.2: Hierarchical representation of the scope definition adopted in this thesis.

(χ^2), *Strict Avalanche Criterion* (SAC), *Bit Independence Criterion* (BIC), *BIC considering the Strict Avalanche Criterion* (BIC-SAC), *BIC considering nonlinearity* (BIC-NL), *Number of Pixel Change Rate* (NPCR), *Unified Average Changed Intensity* (UACI), and *Peak Signal-to-Noise Ratio* (PSNR), is left for future work.

From a security evaluation perspective, this work does not aim to provide a comprehensive cryptographic analysis of the proposed CB-SBox or the resulting cipher. Instead, the assessment is limited to the initial steps of linear and differential cryptanalysis, namely the evaluation of LAP and DAP. A deeper investigation, including *National Institute of Standards and Technology* (NIST) *Special Publication 800-22* (SP800-22), *Majority Logic Criteria (statistical tests)* (MLC), *Chosen-Plaintext Attacks* (CPA), *Known-Plaintext Attacks* (KPA), *Chosen-Ciphertext Attacks* (CCA), and *Brute-Force Attacks* (BFA), as well as full cryptanalytic attacks and resistance evaluations under advanced adversarial models, is beyond the scope of this thesis and is left for future work.

This work does not include comparative evaluations against standardized block ciphers such as *Advanced Encryption Standard* (AES) and *Data Encryption Standard* (DES), or other complete encryption schemes. The objective is not to benchmark the proposed CB-SBox within fully specified cryptographic algorithms, but rather to analyze its properties and performance as an isolated nonlinear component. Furthermore, applications in cryptocurrency and blockchain systems are not considered within the scope of this thesis. Comprehensive comparisons within full cipher architectures and deployment in real-world cryptographic systems are beyond the scope of this thesis and are left for future work.

1.7 Chapter Organization

This thesis is organized as follows.

Chapter 1, entitled **Introduction**, with the subtitle *Framing the Research Problem and Outlining the Path Forward*, and featuring the inspirational phrase "*Learning never exhausts the mind.*" by Leonardo da Vinci (☆ 1452, † 1519), presents the introductory elements of this thesis, including the contextualization of the study, the research problem and hypotheses, motivation, justification, research objectives,

as well as its scientific contributions and scope.

Chapter 2, entitled **Theoretical Framework**, with the subtitle *Theoretical Foundations of Cryptography and Chaos*, and featuring the inspirational phrase "*The important thing is not to stop questioning. Curiosity has its own reason for existing.*" by Albert Einstein (☆ 1879, † 1955), presents the principles and primitives employed in cryptography, including symmetric and asymmetric encryption, stream and block ciphers, digital signatures, key establishment protocols, cipher strength, and cryptanalysis. It also introduces the fundamental aspects of chaos theory, including its scientific foundations, characteristic properties, and representative examples of chaotic maps and systems.

Chapter 3, entitled **State-of-the-Art**, with the subtitle *A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems*, and featuring the inspirational phrase "*If I have seen further, it is by standing on the shoulders of giants.*" by Isaac Newton (☆ 1643, † 1727), presents a novel SLR on chaos-based cryptography, highlighting seminal works and the SOTA that delineate the current frontier of knowledge in this field. This SLR builds upon a preceding SoS that identified the absence of comprehensive SLRs addressing the application of chaos-based S-Boxes in cryptographic systems, thereby constituting an original contribution of this thesis.

Chapter 4, entitled **Materials and Methods**, with the subtitle *From Concept to Implementation: The Path of Scientific Construction*, and featuring the inspirational phrase "*Science is a way of thinking much more than it is a body of knowledge.*" by Carl Sagan (☆ 1934, † 1996), presents the methodological framework and experimental setup supporting the development and evaluation of the proposed chaos-based cryptographic architecture. It details the hardware and software resources employed throughout the study, followed by a comprehensive description of the adopted methodology, including the criteria for evaluating and selecting chaotic maps suitable for cryptographic applications.

Chapter 5, entitled **Experimental Results**, with the subtitle *Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives*, and featuring the inspirational phrase "*Experiment is the sole judge of scientific truth.*" by John Bardeen (☆ 1908, † 1991), presents the design and digital implementation of the proposed

CB-SBox, which constitutes the second contribution of this thesis. The proposed CB-SBox is implemented following the guidelines described in Chapter 4. Its performance is evaluated using metrics related to hardware resource utilization, power consumption, and security. Finally, this chapter presents the integration of the proposed CB-SBox into a Feistel-type cipher, whose output histogram is analyzed to illustrate the practical advantages of the chaos-based design in secure cryptographic applications.

Chapter 6, entitled **Conclusions**, with the subtitle *Reflecting on Achievements and Future Directions in Chaos-Based Cryptography*, and featuring the inspirational phrase "*The end of all our exploring will be to arrive where we started and know the place for the first time.*" by Thomas Stearns Eliot (☆ 1888, † 1965), concludes this thesis by outlining the timeline of activities carried out during the *Doctor of Philosophy* (PhD) research conducted within the *Graduate Program in Electrical Engineering - Programa de Pós-Graduação em Engenharia Elétrica* (PPGEE) at *Federal University of Amazonas - Universidade Federal do Amazonas* (UFAM). It then summarizes the main contributions of this work, followed by a discussion of potential directions for future research.

Chapter 2

Theoretical Framework

Theoretical Foundations of Cryptography and Chaos

"The important thing is not to stop questioning.

Curiosity has its own reason for existing"

Albert Einstein (☆ 1879, † 1955)

2.1 Cryptography Principles

Ensuring information security remains a critical priority in today's increasingly interconnected digital landscape. The proliferation of cyber threats demands robust and adaptive security measures to safeguard sensitive data and systems [64]. Fundamentally, information security is grounded in three core pillars: confidentiality, integrity, and availability. Confidentiality restricts data access to authorized entities; integrity preserves the accuracy and completeness of information; and availability ensures reliable and timely access to data when required [65]. Among various security mechanisms, encryption plays a pivotal role in ensuring confidentiality. In particular, encryption addresses three key dimensions. First, in data protection, it secures data during transmission, rendering it unintelligible to unauthorized users [66]. Second, in communication security, it enhances the robustness and efficiency of communication systems [64]. Finally, in practical applications, encryption enables secure online transactions, supports digital currencies, and protects personal data across diverse communication networks.

2.1.1 Cryptographic Building Blocks

Various cryptographic building blocks are used to support information security. Stream ciphers generate keystreams from internal state machines, commonly based on *Feedback Shift Registers* (FSRs). *Linear Feedback Shift Registers* (LFSRs) are adopted due to their simple structure and low implementation cost, making them suitable for resource-constrained environments such as *Internet of Things* (IoT) devices and satellite communications. However, to overcome the predictability and structural weaknesses inherent in the linearity of LFSRs, *Nonlinear Feedback Shift Registers* (NLFSRs) introduce increased complexity and improved randomness. For instance, combining LFSRs with nonlinear mechanisms or cellular automata further enhances security and the statistical properties of the generated sequences [67].

The advantages of stream ciphers include efficient hardware and software implementations, suitability for low-power devices, and support for real-time encryption. These characteristics make them particularly appropriate for applications such as *Radio Frequency Identification* (RFID) systems and secure sensor networks. Additionally, techniques such as masking power consumption in FSRs improve resistance to power analysis attacks, thereby strengthening robustness against *Side-Channel Attacks* (SCA) [68].

However, certain limitations remain. The vulnerability of LFSRs to cryptanalytic attacks due to their linear structure poses significant security risks unless complemented by nonlinear enhancements. Furthermore, practical implementation challenges, including susceptibility to SCA and the need for optimized compilation and hardware design strategies, require specialized expertise and careful resource management [69].

Block ciphers secure plaintext by dividing it into fixed-length blocks and applying complex encryption algorithms. Among the most prominent are Feistel-based ciphers such as DES, which employ iterative structures to enhance security. For instance, DES uses 16 rounds of the Feistel structure to achieve confusion, typically implemented through nonlinear substitutions via S-Boxes, which obscure the relationship between the ciphertext and the encryption key. Diffusion is achieved using *Permutation-Boxes* (P-Boxes), which apply permutation and mixing operations to

ensure that the influence of a single plaintext bit propagates across multiple ciphertext bits. Modes of operation, such as *Electronic Codebook* (ECB), *Cipher Block Chaining* (CBC), and *Counter Mode* (CTR), enable block ciphers to process data of arbitrary length [70].

The advantages of block ciphers include their versatility and strong theoretical foundations. They are well suited for a wide range of applications, from file encryption to secure communication protocols. Advanced structures such as *Generalized Feistel Networks* (GFNs) and SPNs further improve performance and security, particularly in lightweight cryptographic systems designed for IoT and other resource-constrained environments [71].

However, block ciphers also present disadvantages, including significant computational requirements and vulnerabilities to specific cryptanalytic techniques, such as linear and differential cryptanalysis, as well as fault-based attacks. For instance, Feistel-based systems may require a large number of rounds to achieve sufficient diffusion, which can increase energy consumption in lightweight applications [72].

Hash functions are cryptographic primitives that ensure data integrity by generating fixed-size digests from variable-length inputs. These functions are generally categorized as either *Modification Detection Codes* (MDC) or *Message Authentication Codes* (MAC). MDC schemes, such as *Message Digest Algorithm 5* (MD5) and *Secure Hash Algorithm* (SHA)-1, ensure data integrity by enabling verification of modifications through hash comparisons, whereas MAC schemes, such as *Hash-based Message Authentication Code* (HMAC), combine hash functions with secret keys to provide both integrity and authentication. This makes MAC schemes particularly suitable for secure communications where tamper detection and origin authentication are required.

Hash functions are characterized by computational efficiency in detecting data modifications and by determinism, producing identical outputs for identical inputs. Their cryptographic properties make the inversion of the original input computationally infeasible under standard assumptions. These properties are essential in applications such as password storage, where hashed values protect user credentials, and blockchain systems, which rely on hashing to ensure tamper-resistant transaction records.

However, hash functions also have limitations, including susceptibility to collision attacks and the inability to provide confidentiality. Therefore, they must be combined with encryption mechanisms when secure and confidential communication is required [73].

Digital signature techniques are employed to verify the authenticity and integrity of digital messages, using schemes such as *Rivest–Shamir–Adleman* (RSA), *Digital Signature Algorithm* (DSA), and the *Fiat–Shamir Transformation* (Fiat-Shamir). RSA is widely adopted due to its broad deployment and straightforward implementation, whereas DSA offers improved efficiency in the signature generation process. The Fiat-Shamir transformation, which converts identification schemes into digital signature schemes, is particularly efficient for forward-secure applications. These schemes protect against unauthorized modifications but remain vulnerable to threats such as SCA and key compromise, requiring careful parameter selection.

Digital signatures provide non-repudiation, scalability, and reliable verification mechanisms. Advanced algorithms such as *Elliptic Curve Digital Signature Algorithm* (ECDSA) reduce computational overhead, making them suitable for resource-constrained environments such as IoT [74]. However, these techniques still require significant computational resources and remain susceptible to cryptanalytic attacks, particularly in the case of legacy schemes such as RSA. These challenges highlight the need for alternative approaches that are resistant to emerging quantum computing threats, such as lattice-based cryptography [75].

Key establishment protocols are techniques used to securely establish cryptographic keys between communicating parties, employing both symmetric and asymmetric cryptographic methods. Key transport mechanisms rely on pre-generated keys that are securely transmitted over a communication channel, typically using asymmetric encryption algorithms such as RSA, whereas key agreement methods enable parties to collaboratively derive a shared secret, as exemplified by Diffie–Hellman protocols. Secret-sharing schemes, such as Shamir’s scheme, distribute key material into multiple fragments to enhance resilience against compromise.

Key establishment protocols provide confidentiality and integrity in secure communications. Protocols such as *Datagram Transport Layer Security* (DTLS) optimize symmetric key establishment to improve efficiency and scalability in con-

strained devices [76]. However, key establishment protocols remain vulnerable to man-in-the-middle attacks and often rely on secure initial authentication assumptions. In addition, asymmetric-based protocols, while secure, may introduce significant computational overhead, making them less suitable for low-power devices [77].

2.1.2 Cryptanalysis and Security Evaluation

Evaluating the strength of a ciphertext involves various methods to assess its robustness and statistical randomness. The NIST SP800-22 Statistical Test Suite evaluates randomness using metrics such as frequency, runs, and block frequency tests [46]. Entropy analysis measures unpredictability, where higher entropy indicates stronger ciphertext properties [78]. Autocorrelation functions are used to verify the absence of statistical dependencies within ciphertext sequences. The BIC ensures that each ciphertext bit is uniformly influenced by plaintext and key bits, while the avalanche effect measures whether small changes in the plaintext or key result in significant alterations in the ciphertext.

Resistance to differential and linear cryptanalysis evaluates the cipher’s robustness against structured attacks by analyzing input–output relationships. Key sensitivity tests verify that minor modifications to the secret key lead to substantial changes in the ciphertext, ensuring strong diffusion and confusion properties. Together, these methods provide a comprehensive assessment of cryptographic strength and security [79].

Cryptanalysis is the science of analyzing and breaking cryptographic systems by exploiting weaknesses in their design, implementation, or usage. It involves a variety of techniques aimed at compromising encryption algorithms to recover plaintext or secret keys. A BFA is the most straightforward approach, involving exhaustive testing of all possible keys until the correct one is found; however, it requires significant computational resources. Differential cryptanalysis examines ciphertext differences to infer information about the secret key, whereas linear cryptanalysis uses linear approximations of cryptographic transformations to achieve the same objective. SCA attacks exploit physical leakages such as power consumption or timing variations in electronic circuits, including microchip-level implementations. Algebraic attacks formulate cryptosystems as systems of equations and attempt to

solve them to recover secret keys. Integral cryptanalysis analyzes cipher structures using carefully chosen sets of inputs, while meet-in-the-middle attacks reduce the complexity of exhaustive search in multi-layer encryption schemes, such as double or triple encryption.

CPA and CCA attacks exploit adversary-controlled or adaptively chosen inputs to identify structural weaknesses, while KPA attacks rely on known plaintext–ciphertext pairs. Emerging quantum cryptanalysis leverages algorithms such as Shor’s algorithm to threaten classical public-key cryptosystems, while cryptanalytic time–memory trade-offs accelerate key search processes through precomputation techniques, such as rainbow tables. Fault injection attacks deliberately introduce errors into cryptographic computations to extract sensitive information, whereas dictionary attacks rely on precomputed sets of likely passwords or keys to compromise weak credentials.

2.1.3 Cryptographic Systems and Applications

Cryptographic applications are not limited to secure communication between parties and are now widely used in decentralized systems such as blockchains and cryptocurrencies [80,81]. They rely mainly on hash functions and digital signatures to ensure data integrity, authenticity, and resistance to tampering. Each block stores a hash of the previous one, forming a chain of records in which modifications become easily detectable [80]. Consensus mechanisms, such as Proof-of-Work and Proof-of-Stake, use hashing to support the validation of transactions and the addition of new blocks without relying on a central authority. In cryptocurrencies such as Bitcoin, public-key cryptography enables ownership control and transaction authorization through digital signatures. Together, hashing, signatures, and consensus protocols establish a distributed trust model [81].

The book “Wall or Saturation?: Physical Constraints on Scaling Exact Computation” [82] provides an additional perspective on BFAs in cryptocurrency systems. It interprets Bitcoin as a global-scale secure computational process in which mining transforms energy into entropy, yielding an asymmetry where block generation is computationally expensive while verification remains efficient [80]. Within this framework, proof-of-work ensures ledger consistency, whereas digital signatures

guarantee ownership through the computational infeasibility of private key recovery. Consequently, mining protects consensus: “...it is not a cryptographic attack.”; while digital signatures protect ownership: “...key search is a race against entropy.” [82].

The theoretical age of the universe is approximately 1.38×10^{10} years. Under this perspective, brute-forcing a single Bitcoin private key would require a time horizon on the order of 10^{41} times longer than the age of the universe [82]. Such magnitudes are difficult to grasp in purely computational terms; however, they can be illustrated through physical systems. For instance, the *Googol Gear Machine*, developed by *Daniel de Bruin*, is a mechanical device designed to represent the magnitude of a googol (10^{100}), a number that exceeds typical estimates of the number of atoms in the observable universe. It consists of 100 interconnected gears, each with a reduction ratio of 10:1, resulting in an overall ratio of 10^{100} . Consequently, the first gear must complete a googol rotations for the final gear to rotate once [83]. In other words, if the first gear rotates at 1 Hz, the 18th gear would require approximately the age of the universe to complete a single rotation.

2.2 Chaos Theory

In physics and classical mechanics, chaos refers to a type of dynamical behavior that arises from deterministic equations and exhibits strong sensitivity to initial conditions. This sensitivity renders long-term prediction effectively impossible, capturing the scientific essence of chaos. Beyond its scientific scope, the concept of chaos also holds deep historical and cultural significance. In Hesiod’s *Theogony*, Chaos is portrayed as the primordial entity preceding Gaia, Tartarus, and Eros, a perspective later echoed by Publius Ovidius Naso in *Metamorphoses* [84]. Similarly, the Bible describes chaos as a formless and void state of disorder that opposes divine order, with vivid imagery in Jeremiah 4:23–26 depicting trembling mountains, desolate cities, and a lifeless Earth enveloped in darkness.

Across cultures, myths and philosophical narratives have explored chaos as both a destructive and transformative force. An ancient Chinese account from *The Complete Works of Chuang Tzu* recounts the story of Hun-tun (Chaos), a benevolent emperor of the central region who is unintentionally killed by Shu (Brief) and Hu

(Sudden) when they attempt to endow him with human-like faculties by boring seven openings into his body. These narratives illustrate chaos as a multifaceted concept that bridges science, mythology, and human imagination, symbolizing both unpredictability and the latent potential inherent in disorder [85].



Figure 2.1: Visualization of the Mandelbrot set, a well-known fractal illustrating chaotic behavior in dynamical systems. Source: HypeScience, accessed May 30, 2025.

2.2.1 Scientific Principles

The historical study of chaos requires examining not only its ancient conceptual roots but also its scientific foundations, which were established by pioneers such as Maxwell, Lyapunov, and Poincaré. These scientists recognized the inherent instability in classical mechanics long before modern chaos theory emerged in the 1970s. Their insights laid the foundation for this important field.

In 1873, Maxwell [86] challenged the metaphysical dogma that identical antecedents always produce identical consequences, noting that identical antecedents rarely occur in reality. He observed that physics shifts this principle from sameness to similarity, moving from absolute precision to rough approximation. While this

shift often suffices, Maxwell identified cases where complex instability disrupts predictability. He proposed the existence of unstable systems whose behaviors might conflict with the general postulate of causality, hinting at the chaotic dynamics central to modern physics [87].

Henri Poincaré, widely regarded as a founding figure in modern nonlinear dynamics, revolutionized the study of classical mechanics and mathematics by introducing fundamental concepts and methods such as qualitative analysis of dynamical systems, topology, and early ideas related to bifurcation and ergodic behavior, all of which are central to modern chaos theory. In his 1903 book *Science and Method* [88], Poincaré stated:

"If we knew exactly the laws of nature and the situation of the universe at the initial moment, we could predict exactly the situation of that same universe at a succeeding moment. But even if it were the case that the natural laws had no longer any secret for us, we could still only know the initial situation approximately. If that enabled us to predict the succeeding situation with the same approximation, that is all we require, and we should say that the phenomenon had been predicted, that it is governed by laws. But it is not always so; it may happen that small differences in the initial conditions produce very great ones in the final phenomena. A small error in the former will produce an enormous error in the latter. Prediction becomes impossible, and we have the fortuitous phenomenon." [88]

This passage provides a fundamental basis for understanding chaotic systems, in which small variations in initial conditions can lead to significantly divergent outcomes. Poincaré also investigated the long-term stability of the solar system, questioning whether planetary orbits remain bounded or may eventually diverge. This inquiry led him to the study of the three-body problem, which concerns determining the motion of three celestial bodies—such as the Sun, Earth, and Moon—based on their initial conditions under Newtonian gravitation. Despite its seemingly simple formulation, the problem proved to be highly complex, and Poincaré showed that its solutions exhibit sensitive dependence on initial conditions, preventing reliable

long-term prediction. Although this result received limited attention at the time, it was later recognized as a seminal contribution to the foundations of chaos theory.

Harold Marston Morse and G. D. Birkhoff extended Poincaré’s legacy by advancing the theory of dynamical systems. In 1921, Morse demonstrated the existence of recurrent geodesics of discontinuous type, which are consistent with modern notions of chaotic trajectories. He further constructed a dynamical system exhibiting non-periodic behavior:

“There exists an unending set of symbols, each of which is either 1 or 2, forming a set that is recurrent without being periodic.” [89]

In 1922, Birkhoff [90] classified the motions of dynamical systems into seven categories, including recurrent motions of the discontinuous type. Together with P. Smith, he introduced the concept of metric transitivity, a cornerstone of ergodic theory later employed by R. L. Devaney in the formal definition of chaos. In the 1920s, Van der Pol and Van der Mark observed frequency demultiplication in studies of relaxation oscillations, identifying period-doubling bifurcations in a physical system, now recognized as a fundamental route to chaos. The English mathematicians M. L. Cartwright and J. E. Littlewood investigated nonlinear second-order differential equations and identified the so-called “bad curve.” This work was later extended by Levinson [91], who demonstrated the existence of an attracting solution with chaotic characteristics and a continuum of frequencies.

The immediate precursors of chaos theory, which began to take shape in the 1970s, emerged from two major developments in the early 1960s: Edward Lorenz’s weather model for dissipative systems and the *Kolmogorov-Arnold-Moser* (KAM) theorem for conservative systems. Lorenz [6] introduced a simple system of ordinary differential equations that gives rise to a butterfly-shaped attractor, later termed a “strange attractor” in 1971. This attractor became a central symbol of chaos theory. Lorenz’s model demonstrated that small variations in initial conditions can lead to significantly different outcomes, capturing the essence of chaotic dynamics. His findings in meteorology provided a canonical example of unpredictability in deterministic systems. Further details on Lorenz’s contributions are provided in Section 2.3.

At the International Congress of Mathematicians in 1954, held at the Amsterdam Concertgebouw, Kolmogorov delivered the lecture “The General Theory of Dynamical Systems and Classical Mechanics” [92]. His student Vladimir Igorevich Arnold [93] subsequently provided rigorous proofs of key aspects of this theorem, followed by further contributions from Jürgen Kurt Moser [94], giving rise to the KAM (Kolmogorov–Arnold–Moser) theorem. Kolmogorov’s lecture addressed the persistence of quasi-periodic motions confined to invariant tori in conservative (Hamiltonian) dynamical systems, particularly under small, non-integrable perturbations of the Hamiltonian. These quasi-periodic motions, which lie between regular and chaotic behavior, were already known in Liouville-integrable systems; however, Kolmogorov investigated their structural stability under perturbations. In general, sufficiently small perturbations preserve a set of invariant quasi-periodic tori with positive measure in phase space and on constant-energy hypersurfaces.

In 1969, G. H. Walker and J. Ford [95] applied KAM theory to explain stochastic behavior in conservative nonlinear systems, establishing connections between KAM theory and Poincaré’s earlier results. They showed that violations of KAM conditions can lead to the breakdown of invariant tori, thereby giving rise to chaotic and stochastic dynamics in classical mechanics, effectively bridging abstract mathematical theory with observable physical behavior [85].

2.2.2 Chaos Properties

Chaotic systems are inherently complex. They are dynamical systems in which the next state depends on the current state, making them time-varying rather than static. They are also nonlinear, with properties that cannot be accurately modeled using linear equations. The degree of complexity depends on the level of detail required to represent the system.

There are ten general characteristics of chaotic motion: determinism, non-linearity, sensitive dependence on initial conditions, non-periodicity, some stability with some tension and boundedness, ergodicity, bifurcation, fractional dimensionality, linear behavior in a Lyapunov plot of the distance between trajectories, and finally, the restriction that the initial points of the first return map on a Poincaré section always lie above a line at a 45-degree angle to the horizontal.

Theoretically, the study of chaotic motion within the classical framework of continuous-time autonomous systems requires at least three **deterministic** differential equations without stochastic terms. Consequently, the system states in the past, present, and future are governed by deterministic rules and can be computed through numerical simulation based solely on the system parameters and initial conditions. However, the emergence of stochastic-like behavior in fully deterministic chaotic systems was a surprising result that motivated extensive research in chaos theory. This property is also responsible for the useful characteristics of chaotic systems when applied to communication systems, such as cryptography. It is worth noting, however, that discrete-time maps, such as the logistic map, can exhibit chaotic behavior even in one-dimensional systems.

Chaotic systems are inherently nonlinear, and their governing equations typically involve recursive and higher-order nonlinear terms. This implies that such systems may include expressions such as bx^2 , $4mxy$, y^2z^3 , and $|y|$, where x , y , and z are variables and b and m are constant parameters. Other forms of **nonlinearity** can be more complex, such as the logarithmic voltage–current relationship of a diode or the nonlinear behavior of resistive elements used in analog implementations of Chua’s circuit, as will be discussed in Chapter 2.6. Chaos necessarily arises from nonlinear systems; however, nonlinearity alone does not imply chaotic behavior. Even a naturally chaotic nonlinear system may lose its chaotic regime depending on parameter variations, which can be induced by external factors such as temperature, aging, or parasitic capacitance.

Generally, the evolution of a dynamical system depends on its initial state, even though different systems can exhibit the same final states. When focusing on the entire dissipative attractor, the evolution appears independent of its initial states because all trajectories converge onto the attractor. However, when examining the internal structure of the strange attractor, one observes a peculiar behavior: trajectories both diverge and converge exponentially. **Sensitive Dependence on Initial Conditions** is often referred to as the Butterfly Effect:

“The flapping of a single butterfly’s wing today produces a tiny change in the state of the atmosphere. Over a period of time, what the atmosphere actually does diverges from what it would have done. So, in a month’s

time, a tornado that would have devastated the Indonesian coast does not happen. Or maybe one that was not going to happen, does.” [96]

This illustrates why, despite the existence of modern machines with vast computational power, it is impossible to predict phenomena such as hailstorms, natural disasters, and stock market crashes in advance, regardless of the best efforts to model them accurately. Basically, this means that in real life, it is almost impossible to predict behavior: one can at best make an educated guess and may even be right in most situations, but can never be 100% certain.

A defining property of chaotic systems is their **non-periodicity**, which constitutes a distinct topological form of motion. In chaotic dynamics, orbits are fundamentally non-periodic, meaning they do not repeat their exact trajectory nor intersect previous states in phase space. This characteristic underscores the inherent unpredictability and uniqueness of chaotic systems, distinguishing them from more regular forms of motion.

However, it is important to note that non-periodicity alone does not imply chaos. For example, quasi-periodic motions are also non-periodic but lack the defining features of chaotic behavior. Quasi-periodic systems, such as those described by a simple pendulum with multiple incommensurate frequencies, exhibit deterministic yet non-repeating trajectories that remain geometrically regular.

Conversely, chaotic systems may exhibit transient or parameter-dependent periodic behavior. For instance, the Lorenz system can present periodic windows within an otherwise chaotic regime, where stable limit cycles coexist with strange attractors under specific parameter configurations. This phenomenon, often referred to as intermittency, is commonly observed in fluid dynamics, electronic circuits, and biological systems, where the dynamics may alternate unpredictably between periodic and chaotic phases. This duality highlights the intricate interplay between order and disorder in nonlinear dynamical systems.

The non-periodicity of chaotic systems therefore reflects both their complexity and their sensitivity to parameter variations, while also revealing connections to more structured dynamical regimes. Understanding this interplay is relevant in fields ranging from meteorology and astrophysics to secure communications and cryptographic systems, where chaotic behavior may be either a challenge or a resource.

There are different perspectives on the role of stability in chaotic systems. From a purely mathematical standpoint, chaos is often defined without explicit consideration of orbital stability, since the mathematical framework prioritizes abstract properties such as topological transitivity and sensitive dependence on initial conditions over physical constraints. However, from a physical perspective, stability is essential and must be incorporated into any operational interpretation of chaotic motion.

In this context, chaotic dynamics are typically understood as a **bounded phenomenon** characterized by a form of **dynamical (or weak) stability**. This implies that, although motion on a strange attractor exhibits local instability—leading to exponential divergence of nearby trajectories within finite regions—the system remains globally confined in phase space, preventing divergence to infinity and ensuring long-term bounded evolution.

As Lorenz noted, “A chaotic system is bounded and deterministic, yet unpredictable,” emphasizing that chaos arises from the coexistence of deterministic evolution with practical unpredictability [97]. This interplay between **local instability and global boundedness** is a defining feature of chaotic systems, reflecting the balance between sensitive microscopic divergence and macroscopic structural coherence in nonlinear dynamics.

Ergodicity [98] describes the long-term statistical behavior of a dynamical system. A system is considered ergodic [99] if, over sufficiently long time evolution, its trajectories explore the accessible region of phase space consistent with conserved quantities, such that time averages coincide with ensemble averages [100]. In this sense, ergodicity provides a link between deterministic dynamics and statistical descriptions, connecting individual trajectories to macroscopic observables: although short-term behavior may be unpredictable in chaotic systems, long-term averages can exhibit well-defined statistical regularities.

Importantly, ergodicity does not imply randomness; rather, it reflects a structured and typically uniform exploration of phase space. It ensures that trajectories are not confined to a proper subset of the accessible state space but instead densely sample it over time, subject to the system’s invariants. For instance, in chaotic pendula or turbulent fluid flows, ergodic behavior enables meaningful predictions of

average quantities such as energy or temperature distributions, even when instantaneous motion is highly irregular.

However, not all chaotic systems are ergodic. Ergodicity requires the absence of invariant subsets of positive measure in phase space, meaning that trajectories must not be restricted to periodic or quasi-periodic attractors or invariant manifolds. Consequently, a system may exhibit sensitive dependence on initial conditions and still fail to be ergodic if its phase space decomposes into dynamically isolated regions.

In chaotic systems, the transition to chaos is typically associated with an infinite cascade of **bifurcations** [101], a phenomenon in which increasingly complex dynamical behaviors emerge as system parameters are varied [100]. These bifurcations are characterized by a universal constant $\delta = 4.66920\dots$, known as the Feigenbaum constant. This constant δ plays a role in chaos theory analogous to that of $\pi = 3.14159\dots$ in geometry or $e = 2.71828\dots$ in exponential growth processes, such as radioactive decay. The Feigenbaum constant δ provides a universal scaling factor describing how period-doubling bifurcations accumulate, thereby offering a mathematical framework for understanding the transition from order to chaos [100, 102].

Mitchell Feigenbaum [103], while working at Los Alamos National Laboratory, discovered this constant in the study of nonlinear iterated maps, such as those modeling population dynamics, which exhibit transitions from periodic to chaotic behavior. He showed that a specific ratio governs the convergence rate of successive bifurcation intervals. More precisely, if $L(n)$ denotes the parameter value at the n^{th} bifurcation, then

$$\delta = \lim_{n \rightarrow \infty} \frac{L(n) - L(n-1)}{L(n+1) - L(n)} \quad (2.1)$$

This result reveals a remarkable universality: the same constant emerges across a broad class of dissipative systems undergoing period-doubling routes to chaos. Feigenbaum's contribution thus established a fundamental link between nonlinear dynamics and universal scaling laws in chaotic systems.

Fractional dimensionality [104–106] is a fundamental property observed

in many chaotic systems, exemplified by the Lorenz attractor [6], discussed in (2.3), which evolves in a three-dimensional phase space. In this context, fractional dimensionality refers to the fact that the geometric complexity of the attractor can be characterized by a non-integer (fractal) dimension, reflecting its self-similar structure and deviation from classical Euclidean geometry. This behavior indicates that chaotic trajectories are constrained to sets whose effective dimensionality lies between integer values, giving rise to complex scaling properties.

The implications of fractional dimensionality extend beyond theoretical analysis and are relevant in several scientific and engineering applications. For example, fractional calculus tools, such as the Caputo–Fabrizio fractional derivative, have been used to model and analyze nonlinear dynamical systems, including meteorological phenomena and mechanical oscillations, providing improved flexibility in capturing memory and hereditary effects [106]. Furthermore, fractional-order systems may exhibit hyperchaotic behavior and multi-scroll attractors, which have been explored in secure communications and cryptographic applications due to their enhanced dynamical complexity [107]. However, although fractional dimensionality enriches the modeling framework for chaotic systems, it also introduces additional challenges in analysis, control, and numerical implementation, which may affect predictability and practical realization in real-world systems [106].

The phenomenon of sensitive dependence on initial conditions in chaotic systems leads to the rapid divergence of trajectories originating from slightly different initial states. This divergence can be quantitatively analyzed by plotting the distance between these trajectories versus time on a log-log scale, typically revealing a linear relationship during the early stage of divergence. This **linear behavior in the Lyapunov plot** reflects a positive Lyapunov exponent, which characterizes the exponential rate of separation between nearby trajectories [108]. Such a property is fundamental to understanding the stability and long-term predictability of chaotic systems [100].

Furthermore, weakly chaotic systems, where trajectory divergence does not necessarily follow exponential growth, introduce analytical challenges, as they may exhibit sub-exponential separation, complicating the interpretation of Lyapunov exponents [109, 110]. While the linear behavior observed in Lyapunov plots is a

hallmark of classical chaos theory, it is essential to acknowledge that not all dynamical systems conform to this pattern, particularly those governed by weak chaos, where the underlying dynamics deviate significantly from conventional chaotic behavior [110].

The concept of a **Poincaré section** [111, 112], or surface of section, is a standard tool for analyzing trajectories in an n -dimensional phase space by reducing their representation to an $(n-1)$ -dimensional discrete mapping. This is achieved by intersecting the continuous trajectory with a chosen hypersurface (defined by fixing one phase variable or condition), and recording the states each time the trajectory crosses this surface with a consistent orientation. The resulting set of points provides a lower-dimensional description of the system dynamics and is particularly useful for studying chaotic attractors.

In chaotic regimes, the Poincaré section enables the construction of a first return map, where successive intersections are plotted as iterates of a discrete dynamical system. Such maps often reveal structural organization within chaotic motion, including stretching and folding mechanisms characteristic of strange attractors. In some cases, the geometry of the return map reflects local ordering properties of the flow, although this does not imply global periodicity.

The application of Poincaré sections extends beyond theoretical analysis. For example, in nonlinear electronic oscillators and relaxation systems, these sections can be experimentally reconstructed to visualize transitions to chaos, including phenomena such as torus breakdown [111, 113]. Furthermore, modern data-driven approaches, including manifold learning techniques applied to Poincaré-reduced data, can uncover latent topological structures in high-dimensional chaotic flows, improving the characterization of their dynamical organization [112].

2.2.3 Chaotic Systems

While linear systems have historically been a major focus of scientific investigation, nonlinear behavior is far more common in nature. Over the past several decades, extensive research has uncovered and analyzed over forty chaotic systems [1, 7–13], demonstrating their fundamental relevance and intricate dynamics.

In the following paragraphs, five specific chaotic systems and maps (Logistic

Map, Lorenz, Rössler, Linz and Sprott, and Chua) will be discussed. The nonlinear differential (and difference) equations governing these systems and maps will be presented, and their chaotic behavior will be systematically analyzed.

The **Logistic Map** [8, 24, 38, 40, 48] is a canonical discrete-time nonlinear system that illustrates how complex chaotic behavior can emerge from a simple quadratic recurrence driven by a single control parameter. Introduced by Robert May [8], it models population dynamics in environments where growth is constrained by limited resources and environmental carrying capacity.

Initially, assuming a constant growth rate R , the system can be described by the linear difference equation $x_{n+1} = Rx_n$, which leads to three regimes: unbounded growth for $R > 1$, constant population for $R = 1$, and exponential decay for $0 < R < 1$. However, this linear formulation is not biologically realistic, since real populations are subject to saturation effects.

By introducing a state-dependent growth limitation, the model becomes nonlinear and is expressed by the quadratic recurrence in Equation (2.2). This nonlinearity yields a rich bifurcation structure as R varies: extinction for $0 < R < 1$, convergence to a fixed point for $1 < R < 3$, period-doubling oscillations for $3 < R \lesssim 3.57$, and chaotic dynamics for larger values of R [103]. Periodic windows still appear within the chaotic regime, including stable cycles such as period-3 behavior near $R \approx 3.83$. For $R = 4$, the map becomes fully chaotic on $[0, 1]$ for almost all initial conditions, exhibiting strong sensitivity to initial states.

The Logistic Map thus provides a classical illustration of the transition from order to chaos through nonlinear feedback mechanisms.

$$x_{n+1} = Rx_n(1 - x_n) \tag{2.2}$$

Edward **Lorenz** [6, 47, 114, 115], a mathematician and meteorologist at the Massachusetts Institute of Technology (MIT), made seminal contributions to chaos theory in the early 1960s while studying numerical weather prediction. Using a computer model governed by 12 nonlinear differential equations to simulate atmospheric convection, he observed an unexpected phenomenon: when restarting a simulation from intermediate values, he expected the same trajectory, but instead obtained a dramatically different evolution.

Lorenz traced this divergence to numerical precision. The computer stored values with six decimal places, whereas the restart input was rounded to three decimal places. This seemingly negligible perturbation (e.g., 0.506127 versus 0.506) led to exponentially diverging trajectories. This effect, later formalized as *sensitive dependence on initial conditions*, demonstrated that deterministic nonlinear systems can exhibit fundamentally unpredictable long-term behavior due to amplification of infinitesimal perturbations. This result challenged the classical assumption that small changes in initial conditions produce proportionally small changes in outcomes.

By reducing his original 12-equation atmospheric model to a simplified system of three ordinary differential equations, Lorenz preserved the essential nonlinear dynamics while removing direct physical interpretation. Interestingly, this reduced system was later shown to also describe the dynamics of mechanical systems such as a water wheel. The resulting trajectories do not converge to fixed points or periodic orbits; instead, they evolve on a bounded geometric structure known as the Lorenz attractor, characterized by a double-scroll topology. This attractor represents a form of deterministic non-periodic behavior, now recognized as a hallmark of chaotic dynamics [6, 116].

The Lorenz system in Equation (2.3) contains nonlinear interaction terms xy and xz , which are responsible for the system's stretching and folding mechanism in phase space. The dynamics depend on three constant parameters (σ , ρ , and β), and require non-zero initial conditions to generate non-trivial trajectories [114, 115].

$$\begin{aligned}\frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= x(\rho - z) - y, \\ \frac{dz}{dt} &= xy - \beta z.\end{aligned}\tag{2.3}$$

The **Rössler** system [117], named after Otto Rössler, originated from his studies in chemical kinetics [7]. It is described by three coupled nonlinear ordinary differential equations and is structurally simpler than the Lorenz system (2.3), since it contains a single nonlinear term, xz , appearing in the third equation. The Rössler system (2.4) is defined by three state variables x , y , and z , and three constant parameters A , B , and C . Typical parameter values include $A = 0.2$, $B = 0.2$, and $C = 5.7$, with non-zero initial conditions.

The system exhibits qualitatively different dynamical regimes depending on the parameter C . By varying C while keeping A and B fixed, one observes transitions from periodic to chaotic behavior. Rather than analyzing time series alone, phase-space projections (e.g., the x - y plane) provide clearer insight into the attractor structure. For $C = 2.5$, the system exhibits a period-one limit cycle. At $C = 3.5$, it transitions to a period-two orbit, and at $C = 4.0$, it displays period-four behavior. These period-doubling bifurcations constitute a classical route to chaos. For $C = 5.7$, the system enters a chaotic regime characterized by bounded but aperiodic trajectories.

Further characterization can be obtained from the time series of the z -variable at $C = 5.7$. In this regime, trajectories spend most of the time near the x - y plane, while intermittent excursions in the z -direction correspond to bursts away from this plane, reflecting the underlying stretching and folding dynamics of the attractor. The Rössler attractor thus provides a canonical example of a simple continuous-time system exhibiting deterministic chaos and serves as a foundational model in nonlinear dynamics and chaos theory.

$$\begin{aligned}\frac{dx}{dt} &= -y - z, \\ \frac{dy}{dt} &= x + Ay, \\ \frac{dz}{dt} &= B + z(x - C).\end{aligned}\tag{2.4}$$

A necessary but not sufficient condition for the emergence of chaos in a dynamical system is the presence of nonlinear terms in its governing equations. In the Logistic Map (2.2), the nonlinearity is introduced by the quadratic term x_n^2 . In the Lorenz system, nonlinearities arise from the bilinear coupling terms xz and xy . Similarly, in the Rössler system, the term zx in the third differential equation introduces nonlinearity.

In all these systems, the nonlinear terms are primarily realized through multiplicative interactions between state variables, which are computationally more expensive in digital hardware implementations than linear operations. This observation motivates the investigation of whether nonlinearities can be reformulated or approximated to improve implementation efficiency in hardware-oriented chaotic systems.

Linz and Sprott [11] conducted an extensive numerical search for an algebraically simplest chaotic system that weakens the NL to an absolute form, $|x|$. They identified a system, described by equation (2.5), which exhibits chaotic dynamics for $A = 0.6$ and $B = 1$, with the parameter $B = 1$ influencing solely the attractor's size.

Chaos persists even for arbitrarily small values of B , although both the attractor and its basin of attraction decrease proportionally in size. Additionally, chaotic behavior arises when the nonlinear term $|x|$ is generalized to $|x|^n$, for any nonzero exponent n . This system follows a period-doubling route to chaos analogous to that observed in the bifurcation structure of the Logistic Map. This represents the most elementary chaotic flow, with Linz proving that chaos disappears if any term in the defining equations is set to zero.

For $B = 1$, the attractors exhibit different behaviors depending on A : at $A = 0.8$, 0.675 , and 0.644 , the system oscillates without chaotic behavior, with trajectories confined to their respective attractors. However, at $A = 0.6$, the system displays chaotic dynamics, as trajectories explore new regions of the attractor.

$$\begin{aligned}\frac{dx}{dt} &= y, \\ \frac{dy}{dt} &= z, \\ \frac{dz}{dt} &= -Az - By \pm (|x| - 1).\end{aligned}\tag{2.5}$$

Chua's circuit family [10, 118] is a class of simple analog electronic circuits capable of exhibiting a wide range of nonlinear and chaotic phenomena, including period-doubling routes to chaos, Hopf bifurcations, chaotic regimes consistent with Shil'nikov's theorem, and hidden attractors [13]. This circuit is widely recognized as one of the simplest third-order autonomous electronic systems capable of generating chaos.

It is composed of four linear elements (one resistor, one inductor, and two capacitors) together with a single nonlinear element defined by a piecewise-linear or nonlinear voltage-current characteristic. The circuit dynamics are governed by three coupled nonlinear ordinary differential equations derived from Kirchhoff's laws, where the nonlinearity is introduced through a single state variable.

These equations can be transformed into a dimensionless state-space representation, as shown in Equations (2.6) and (2.7), via appropriate variable normalization, which facilitates both analytical and numerical analysis.

Digital implementations of Chua's circuit offer notable advantages over analog realizations, particularly in the precise control and emulation of circuit elements such as negative resistance, capacitance, and inductance, which facilitates the tuning of parameters to achieve different chaotic regimes.

Numerical and circuit-level simulations have revealed a wide variety of chaotic attractors, with approximately 40 distinct attractor types identified within the Chua's circuit family [119]. Each attractor corresponds to specific parameter configurations, and this diversity highlights the system's ability to generate rich nonlinear dynamics.

For instance, attractor-specific behaviors arise from variations in parameters such as α , β , γ , m_0 , m_1 , and k , enabling systematic exploration of different chaotic regimes.

$$\begin{aligned}\frac{dx}{dt} &= k\alpha(y - x - f(x)), \\ \frac{dy}{dt} &= k(y - x + z), \\ \frac{dz}{dt} &= k(-\beta y - \gamma z).\end{aligned}\tag{2.6}$$

$$f(x) = m_1x + \frac{1}{2}(m_0 - m_1)(|x + 1| - |x - 1|).\tag{2.7}$$

Hyperchaos [50, 60, 120, 121], introduced by Rössler in his 1979 work on higher-dimensional chaotic dynamics [122], extends the concept of classical chaos by incorporating additional degrees of freedom. It is characterized by dynamical systems with at least two positive Lyapunov exponents, in contrast to conventional chaotic systems such as those in Equations (2.3), (2.4), and (2.5), which typically exhibit only one positive Lyapunov exponent.

Hyperchaos is therefore associated with exponential divergence along multiple independent directions in phase space. While classical chaos is defined by sensitiv-

ity to initial conditions and deterministic unpredictability, hyperchaos represents a higher-dimensional form of instability in which multiple expanding directions coexist, significantly increasing the complexity of the system dynamics.

Rössler’s work [122] introduced a four-dimensional dynamical system (Equation (2.8)), described by a set of coupled first-order ordinary differential equations, which demonstrated hyperchaotic behavior with a minimum of four state variables, four integrators, four parameters $(a, b, c, d) = (0.25, 3.00, -0.50, 0.05)$, and a single nonlinear term xz . This formulation addressed limitations of low-dimensional chaotic systems such as the Lorenz attractor (2.3) and the classical Rössler system (2.4), which typically exhibit only one positive Lyapunov exponent.

Hyperchaos can arise naturally in higher-dimensional dynamical systems where the state evolves under multiple simultaneously expanding directions in phase space, leading to more complex and less predictable behavior. This property enables broader applications in nonlinear circuits, secure communications, biological modeling, and fluid dynamics [121, 123]. Hyperchaotic systems generate a richer set of trajectories due to concurrent instabilities in multiple state-space directions, a feature not present in standard chaotic systems.

Rössler’s original hyperchaotic model (Equation (2.8)) was among the first to demonstrate that a minimal four-dimensional continuous-time system can sustain hyperchaotic attractors using relatively simple nonlinear interactions. In such systems, the inclusion of an additional state variable effectively introduces an extra expanding direction in phase space, enabling hyperchaotic dynamics [37].

$$\begin{aligned}\frac{dx}{dt} &= -y - z, \\ \frac{dy}{dt} &= x + ay + w, \\ \frac{dz}{dt} &= b + xz, \\ \frac{dw}{dt} &= -cz + dw.\end{aligned}\tag{2.8}$$

The concept of **Compound Chaos** [124–126] emerged as a formal topic within nonlinear dynamics and chaos theory in the late 20th and early 21st centuries [125, 126]. It refers to the coexistence and interaction of multiple chaotic attractors

within a single dynamical system, resulting in a composite phase-space structure with multiple coexisting dynamical regimes.

This phenomenon typically arises in systems with higher-order nonlinear interactions, where distinct chaotic attractors coexist, interact, or merge into a unified but structurally complex dynamical behavior. In this sense, compound chaos is associated with systems that exhibit not only chaotic motion but also hierarchical or multi-scale attractor organization.

As described by Lu *et al.* [126], such behaviors can be generated by appropriate parameter tuning or structural modifications of classical chaotic systems, leading to attractors with compound or hybrid structures. They further showed that these systems may undergo bifurcations that produce multiple coexisting attractors in phase space, resulting in complex trajectory switching and enhanced dynamical richness.

Further studies indicate that compound chaos often arises in systems with symmetry properties or modular coupling structures, where interactions between subsystems increase overall complexity. In particular, Tiwari *et al.* [124] demonstrated that engineered compound chaotic systems can generate composite attractors with enhanced dynamical features, including increased unpredictability, modified Lyapunov spectra, and intertwined basin structures. These compound attractors exhibit characteristic phase-space properties such as fractal basin boundaries, symmetry-breaking bifurcations, and multistability.

Ahmadi *et al.* [13] extended this concept by proposing a two-dimensional megastable dissipative chaotic system whose nonlinear dynamics are based on trigonometric and hyperbolic functions. The system exhibits a countably infinite set of coexisting attractors, including both self-excited and hidden attractors.

Similarly, Vijayakumar *et al.* [12] introduced a simple three-dimensional autonomous chaotic system featuring a single stable-node equilibrium. Its behavior is governed by the parameter k , which determines transitions between different dynamical regimes. Since the equilibrium point is located at $(k, 0, 0)$, distinct basins of attraction emerge on the plane $x = k$. Two-dimensional phase-space cross-sections in the y - z plane reveal four possible asymptotic behaviors depending on initial conditions: a chaotic attractor, a periodic attractor, a stable fixed point, or unbounded

trajectories.

Chapter 3

State-of-the-Art

A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems

3.1 Chapter Introduction

Chaos theory has become a prominent area of research across multiple disciplines since Lorenz's seminal work in 1963 [6]. Over forty nonlinear differential equations exhibiting chaotic behavior have been reported [1, 7–13], and have found applications in fields such as mechanics [14], biology [15], ecology [16], astronomy [17], and notably cryptography [18–21, 23].

Chaos and encryption are intimately linked through the cryptographic principles of confusion and diffusion [62]. Confusion, typically realized through nonlinear S-Boxes, obscures the relationship between ciphertext and the encryption key, while diffusion, usually implemented via P-Boxes and mixing operations, ensures that a single plaintext bit influences multiple ciphertext bits. Chaotic systems naturally exhibit properties such as sensitivity to initial conditions and ergodicity, which closely correspond to the cryptographic principles of confusion and diffusion, respectively.

Sensitivity to ICs ensures that minimal changes in input, such as slight variations in the key, produce significantly different outputs, enhancing resistance to differential attacks. Ergodicity allows chaotic maps to eventually cover the entire state space, contributing to statistical uniformity in outputs and improving resilience

against cryptanalysis. The inherent complexity of deterministic chaotic maps produces outputs that appear random, providing a balance between reproducibility and unpredictability, which strengthens both confusion and diffusion in cryptographic schemes.

As identified through an exploratory SoS, more than 80% of the existing surveys at the intersection of chaos and cryptography focus on multimedia applications, such as image, audio, and video encryption, thereby leaving a gap in the systematic analysis of block cipher design and S-Box construction within chaos-based cryptography. This paper addresses this gap by conducting the first structured SLR that synthesizes and critically evaluates studies on S-Boxes in the context of chaos-based cryptography.

Following the methodology outlined by [138,139] and supported by the Parsifal online platform (<https://parsif.al/>), the review begins with a SoS to examine existing stand-alone surveys and to define the scope of the original contribution of this SLR. It then extends the analysis to primary studies within the defined scope to identify the current knowledge frontiers in chaos-based S-Box design.

The remainder of this study is organized as follows: Section 3.2 presents a SoS to identify the research gaps addressed by this original SLR. Section 3.3 describes the structure, scope, positioning, and contributions of the present SLR. Section 3.3.2 presents the novel SLR at the intersection of chaos-based cryptography and S-Box construction, discussing design considerations, analyzing pioneering and influential contributions, reviewing recent SOTA works, and concluding with a comprehensive analysis of the conducted SLR. Finally, Section 3.4 summarizes the results of the SoS and SLR studies and highlights directions for future research.

3.2 Survey of Surveys: Literature Positioning

The present research is based on the SLR concepts proposed in [138, 139], which provide a standardized framework for conducting SLRs, originally derived from the health sciences and later tailored to the field of *Information Systems* (IS). After reviewing existing surveys (SoS) as a highly recommended preliminary step, Okoli [139] proposes the following eight-step process:

- (1) Identify the research objectives;
- (2) Develop a protocol, a documented plan to be followed during the SLR to achieve the defined objectives;
- (3) Perform a practical screening of sources, including journals, abstracts, classification criteria, languages, scope, publication years, authors, keywords, and other relevant factors;
- (4) Conduct the literature search across multiple databases, such as *Institute of Electrical and Electronics Engineers* (IEEE), *Multidisciplinary Digital Publishing Institute* (MDPI), Springer, *Association for Computing Machinery* (ACM), Google Scholar, Scopus, *Joint Information Systems Committee* (Jisc), *Web of Science* (WoS), *Bielefeld Academic Search Engine* (BASE), and *COnecting REpositories* (CORE), until no additional relevant studies are identified;
- (5) Extract data in a quantitative and/or qualitative manner;
- (6) Assess the quality of the selected studies, including articles, journals, and theses;
- (7) Synthesize the findings by combining data from different sources, potentially using meta-analysis and supporting software tools; and
- (8) Report the results clearly, documenting all steps followed and addressing the research objectives.

3.2.1 Methodology

Following the preliminary step proposed in [139], this study begins by surveying existing reviews in the same research area (i.e., a SoS). The Parsifal framework (<https://parsif.al/>), which incorporates the *Population, Intervention, Comparison, Outcome and Context* (PICOC) search criteria, is utilized to support this process. The objective is to identify and evaluate existing stand-alone SLRs within the area of chaos-based cryptography. Mapping these reviews clarifies their scope

and quality, highlights research gaps, and assesses whether the available evidence is sufficient to guide further investigations.

Regarding the research protocol, the PICOC criteria are defined as follows: the **Population** comprises literature reviews addressing chaos-based cryptography and information security; the **Intervention** corresponds to the application of encryption primitives and secure communications in chaos-based cryptography; the **Comparison** is not applicable, as the focus is on identifying and analyzing existing stand-alone reviews in chaos-based cryptography, emphasizing their scope, methodologies, and reported gaps; the **Outcome** refers to the identification of existing reviews in terms of number, type, scope, and quality, together with reported gaps and directions for future research; and the **Context** is academic research, focusing on studies published in journals and conference proceedings, with the aim of mapping the current SOTA in chaos-based cryptography reviews.

In addition to the PICOC criteria, the remaining elements of the research protocol are defined as follows: The **research questions** address the identification of stand-alone literature reviews, their types and scopes, the SOTA, reported research gaps, and recommendations for future work. The following **keywords** are employed in the search: academic research (scientific study, peer-reviewed, journal, conference) associated with the Outcome dimension of PICOC; chaos (chaotic, chaos, map, circuit, system, nonlinear, dynamics, behavior, sequence) associated with the Intervention dimension of PICOC; cryptography (encryption, cipher, cryptosystem, secure, data, protection, cryptanalysis, information security, S-Box, algorithms) associated with the Intervention dimension of PICOC; gap (limitation, evidence, future, challenges) associated with the Outcome dimension of PICOC; methodology (protocol, approach, procedure, technique, method, research design, evaluation criteria, methodological) associated with the Outcome dimension of PICOC; and stand-alone literature reviews (review, survey, systematic, mapping, study, scoping, SOTA, literature, narrative, SLR) associated with the Population dimension of PICOC.

The execution of the SoS followed a structured multi-stage process encompassing database selection, study screening, quality assessment, and data extraction. The SoS was conducted across the following scientific databases, listed in order of

relevance to its scope: IEEE, MDPI, WoS, Springer, Google Scholar, Wiley, and ACM. A total of 320 publications were imported into the Parsifal tool, of which 24 were retained after the inclusion-exclusion criteria (IC/EC) phase. This phase evaluated the set of primary studies, the organization of the work through tables and figures, the presence of discussions on research gaps and future directions, the clarity of research objectives, and the extent of comparison among primary studies. Among these 24 publications, 18 achieved scores sufficient to advance to the data extraction phase, as quantitatively illustrated in the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) diagram in Figure 3.1, analyzed in detail in Section 3.2.2 and summarized in Table 3.1 .

3.2.2 Data Extraction

This section presents the data extracted from the 18 surveys selected after the screening and quality assessment phases, focusing on their scope, classification approaches, evaluation criteria, and main contributions. The extracted data are summarized in Table 3.1 at the end of this subsection and provide the basis for the synthesis and comparative analysis presented in Section 3.2.3.

Sadkhan *et al.* [140] present a concise narrative survey on the application of chaos theory in both digital and analog voice encryption. Unlike text and image data, in voice signals the application of confusion and diffusion mechanisms is sufficient to render the speech unintelligible. The surveyed studies are categorized into the following taxonomy, without cross-comparisons: stream ciphers, block ciphers, and public-key cryptography.

In this survey [140], the evaluation parameters for voice encryption include residual intelligibility, verified by human listeners in analog encrypted speech; keyspace, considered an indicator of cryptographic strength; and encryption delay, representing the time required to encrypt a signal segment. The voice encryption techniques are further classified into four groups: conventional methods, namely analog techniques that manipulate the voice signal in time, frequency, and amplitude domains; orthogonal transformations; blind source separation, where the source signal is unobserved; and chaotic systems, classified into amplitude-domain, transform-domain,

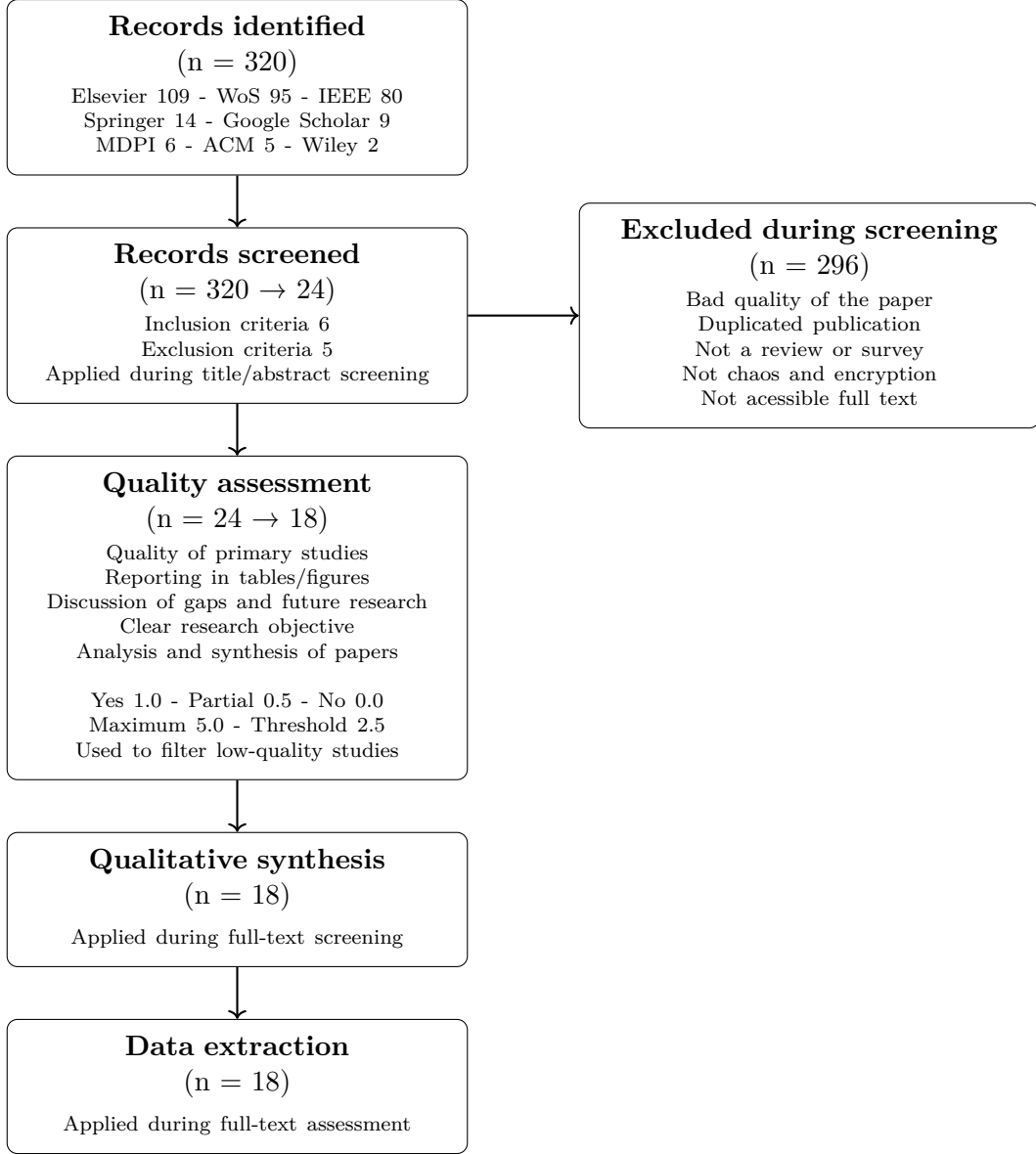


Figure 3.1: PRISMA diagram of study selection in the SoS

and symmetric cryptographic approaches. The authors briefly propose two directions for future research: multi-algorithmic approaches and perturbation techniques to mitigate short cycle lengths.

Hussain and Shah [141] present a tutorial on the use of S-Box in block ciphers. The study discusses 66 definitions, lemmas, theorems, and corollaries, supported by a literature review of 89 papers addressing Boolean functions and S-Box theory, their classes (including three special classes of Boolean functions: bent, semi-bent, and plateaued), and cryptographic properties.

Although the title of the paper in [141] includes the term *chaotic* (which does not appear in the keywords), only 5 of the 49 papers analyzed in the literature re-

view section address the application of chaos theory in the construction of S-Boxes. The study does not include a conclusion section and provides neither recommendations for future research nor an explicit discussion of research gaps in the surveyed literature.

Zhen *et al.* [142] present a brief survey on digital chaos-based cryptography, without restricting the type of data to be encrypted, and trace the development of the field since the 1990s. The narrative review categorizes prior work into four main, non-overlapping taxonomies: *Pseudorandom Number Generator* (PRNG), symmetric cryptosystems (stream and block ciphers), public-key cryptosystems, and hash functions. The survey also identifies four major challenges: (i) deficiencies of chaotic systems, suggesting future research on the design of higher-performance systems for cryptographic applications; (ii) the absence of established security standards, indicating the need for benchmarks tailored to chaos-based cryptography; (iii) finite-precision representation in digital implementations, which often leads to pseudo-chaos and dynamical degradation, thereby requiring techniques such as parameter perturbation or the use of high-dimensional dynamical systems; and (iv) high computational cost, arising from real-number calculations and the large number of iterations required for chaos to emerge.

Shukla *et al.* [143] present a concise review of chaos-based cryptography. A total of 62 papers published between 1993 and 2015 were analyzed according to multiple features, such as security level (e.g., high, medium), cryptanalysis attack prevention (e.g., BFA, KPA), cipher type (e.g., stream, block), application area (e.g., medical, military), space complexity (e.g., low, high), implementation complexity (e.g., complex, simple), techniques employed (e.g., LFSR, PWLCM), efficiency and reliability (e.g., high, low), implementation environment (e.g., MATLAB, FPGA), processing speed (e.g., high, medium), predictability (yes or no), feasibility (e.g., yes, reasonable), accuracy (e.g., high, medium), key length (e.g., large, large enough), cost (e.g., high, medium), and quality assurance (e.g., applicable, medium). The review does not identify research gaps in the field, nor does it provide suggestions for future work.

Fang *et al.* [144] present a SOTA survey in IEEE Communications Surveys & Tutorials journal, covering two decades of research on digital chaotic modulation,

particularly *Differential Chaos Shift Keying* (DCSK), targeting *Ultra-Wide Band* (UWB) wireless applications. The study begins with the fundamental principles and a historical overview of *Chaos Shift Keying* (CSK) and DCSK. It then summarizes the main achievements related to six DCSK variants (FM-DCSK, QCSK, M-ary DCSK, CS-DCSK, DDCSK, and MC-DCSK) and discusses the joint design of DCSK with eight complementary techniques (SIMO FM-DCSK, STBC-DCSK, MIMO Relay DCSK-CD, DCSK-CC, LDPC-Coded DCSK, DCSK-ARQ/CARQ, Network-Coded DCSK, and Other DCSK-Related Systems). The survey concludes by outlining directions for future research, organized into six detailed topics.

Muthu and Murali [145] review 12 surveys in the field of chaos-based image cryptography and identify a research gap related to the evaluation of nonlinear chaotic behavior. Their main contribution is the application of detection techniques to assess the chaotic properties of newly developed maps designed primarily for encryption. The authors employ chaos detection methods to evaluate the chaotic and non-chaotic ranges of 25 discrete and 18 continuous novel chaotic systems. They report that the bifurcation diagram (96%) and Lyapunov exponent (88%) are the most frequently used techniques for discrete chaotic maps, whereas phase portrait (100%), bifurcation diagram (67%), and time series (67%) are the most common for continuous maps. Although the study does not suggest future work, it emphasizes the need for more comprehensive experiments and analyses on novel chaotic maps and systems to develop secure chaos-based image cryptographic systems resistant to various attacks.

Khaleel and Abduljaleel [146] present a concise review of papers published between 2010 and 2020 on chaos-based image cryptography. They describe five primary techniques for image encryption: cellular automata, random grids, transform-based techniques such as *Discrete Wavelet Transform* (DWT) and *Discrete Cosine Transform* (DCT), DNA coding, and chaotic maps. The survey is organized chronologically, summarizing the main characteristics of the papers in a table. The studies are also classified according to six techniques mixed with chaotic maps: DNA, dynamic DNA, cellular automata, transformations, S-Box, and hash functions. Each paper is compared using the following performance parameters: image entropy, NPCR, UACI, keyspace, and correlation (horizontal, vertical, and diagonal). The authors

conclude by suggesting future work that incorporates bioinformatics inputs, such as fingerprints or voiceprints, to dynamically determine the chaotic parameters during algorithm execution, thereby enhancing resistance against attacks.

Haseeb *et al.* [147] present a narrative review of 20 studies published between 2018 and 2022, focusing on speech encryption using chaos-based cryptography. The following main topics are addressed: analog and digital audio, stream ciphers, scrambling, perturbation, masking, shuffling, permutation, one-to-many mapping, pseudo-random bit generation, and DNA coding. Two types of comparisons are conducted: statistical analysis and the types of chaotic maps employed in the studies. The review lacks a discussion of research gaps and directions for future work.

Fang *et al.* [148] conduct a survey across five databases (IEEE, WoS, Google Scholar, ScienceDirect, and arXiv), covering articles published between 2010 and 2022 on chaos-based image encryption, excluding MSc and PhD theses. The review encompasses algorithms based on Arnold transform, quantum systems, compressed sensing, and chaotic systems, including low-dimensional, high-dimensional, fractional-order, and composite ciphers incorporating DNA coding, S-Boxes, block ciphers, deep learning, and other approaches. The study identifies several research gaps for future investigation: (i) security analysis of image encryption algorithms, as there is no established set of international standards to evaluate the security, complexity, and scalability of chaos-based encryption systems; (ii) image encryption algorithms combining chaotic systems with neuromorphic computing; and (iii) image encryption algorithms combining chaotic systems with memristors.

Zia *et al.* [149] present a survey on chaos-based image cryptography techniques. The study analyzes ten prior surveys in the field to define its scope. After defining seven performance parameters (NPCR, UACI, KA, HA, CC, IE, and NA), the survey reviews contributions to chaos-based image cryptography published from 2016 to 2021. These works are categorized into spatial, temporal, and spatiotemporal domains. The spatial domain is further subdivided into three categories: chaos, DNA, and cellular automata. In total, 43 primary studies are reviewed and compared using the seven performance parameters. The survey concludes by emphasizing that the field of image encryption remains in a growth stage, still lacking maturity in terms of security, computational efficiency, and parameter optimization.

It also highlights a research gap regarding the absence of standardized benchmarks for evaluating efficiency and effectiveness. Finally, the authors suggest extending image encryption techniques to video encryption as a direction for future work.

Zolfaghari and Koshiba [150] survey chaos-based image cryptography, including the SOTA of primary studies, the ecosystem in which these studies are situated, and a roadmap of expected future contributions. The study begins by analyzing 19 surveys published between 2014 and 2022 in the areas of image encryption, chaos-based image cryptography, image processing assisted by *Artificial Intelligence* (AI), and image encryption assisted by AI, noting that none of them address the ecosystem of the reviewed studies, and only three address the roadmap for future work.

To organize the SOTA, the survey [150] classifies more than 200 primary studies using a taxonomy comprising three non-overlapping dimensions: chaos (domain, source, and dimension), encryption (symmetric versus asymmetric, block versus stream, and primitives), and image (2D versus 3D, grayscale versus color, and transforms). The ecosystem is characterized by challenges (encrypted image processing, attack protection, and evaluation), application areas (e.g., IoT, medical, and satellite), and enabling technologies (DNA and quantum coding, signal processing, hardware implementation, parallel processing, and fuzzy systems). Regarding the current and future roadmap, the study identifies emerging trends in quantum-inspired AI, bio-inspired AI, and neural networks applied to chaos, image processing, security, image encryption, and chaotic cryptography.

Al-Hazaimeh *et al.* [151] provide a brief survey on chaos-based multimedia cryptography with emphasis on network and Internet security. The background on chaos theory in cryptography highlights four equivalences between chaotic systems and cryptographic algorithms: real numbers versus finite sets of integers, iterations versus rounds, parameters versus keys, and sensitivity versus diffusion. The authors apply a taxonomy for chaotic maps, classifying them into continuous-time (3D) and discrete-time (1D or 2D). The authors review eleven papers published between 2001 and 2022, comparing them based on four security parameters: keyspace, key sensitivity, correlation (horizontal, vertical, and diagonal), and entropy-related metrics (NPCR and UACI). The survey does not identify research gaps and does not suggest future work.

Shraida and Younis [152] published a short survey on chaos-based color image cryptography, available online via the University of Basrah (Iraq) and indexed in Google Scholar. The authors start by reviewing three prior surveys in the field [153–155]. The paper then presents a brief overview of chaos-based image cryptography and introduces several performance metrics: keyspace, key sensitivity, histogram, correlation, information entropy, NPCR, UACI, *Mean Square Error* (MSE), and PSNR. Subsequently, the survey analyzes and compares 22 articles published between 2017 and 2022 in terms of metrics such as keyspace, correlation (horizontal, vertical, and diagonal), information entropy, NPCR, and UACI, using the standard Lena color image as a benchmark. The study concludes without identifying research gaps or suggesting directions for future work. Its reference list includes 37 entries without providing their titles.

Zhang and Liu [156] present a comprehensive review of chaos-based image cryptography, covering its applications and associated challenges. The paper begins with a brief introduction to the field, including both discrete and continuous chaotic systems, their characteristics, and performance indicators. The literature review then proposes a taxonomy that classifies approaches into three categories: symmetric encryption in the spatial and frequency domains, such as block and stream ciphers, DWT, and DCT; asymmetric encryption approaches, such as RSA, *Elliptic Curve Cryptography* (ECC), and chaos synchronization; and other enabling technologies, including neural networks, DNA, blockchain, and cellular automata. The review also discusses evaluation parameters such as keyspace, histogram, correlation, information entropy, UACI, and NPCR; application domains including medical imaging, IoT, and satellite imagery; and key challenges in the field. In addressing these challenges, the review analyzes studies aimed at protecting image-encryption algorithms from attacks and cryptanalysis, as well as processing encrypted images (including compression, retrieval, selective encryption, and thumbnail preservation). The paper concludes by emphasizing that these challenges represent opportunities for future research.

Singh *et al.* [157] submitted in 2020 a SLR, published in 2024, on the use of chaos in three image security techniques: watermarking, steganography, and encryption. A total of 29 papers, published between 2006 and 2019, were selected from

an initial corpus of 499 and analyzed following the PRISMA guidelines. Theoretical papers lacking performance evaluation were excluded. The selected studies were compared across six dimensions: differential attack analysis, measured using NPCR and UACI; keyspace; MSE; PSNR; information entropy; and *Structural Similarity Index Measure* (SSIM). This SLR lacks discussion of reported gaps and recommendations for future research.

Gupta *et al.* [158] present a SOTA review of image cryptographic mechanisms, explicitly comparing their study with five other contemporary SOTA surveys to delineate the scope and emphasize novelty. The review is not limited to chaos-based cryptography; it also encompasses diverse encryption techniques, including DNA, ECC, deep learning, and hybrid approaches. Among these, chaos-based cryptography was the most prevalent (34%) in the literature, indicating its widespread adoption in recent years. To structure the analysis, the authors propose a novel taxonomy, categorizing the 134 surveyed papers into 13 distinct groups to facilitate systematic comparison. Each group is examined in terms of key concepts, performance evaluation, cryptanalysis metrics, and authentication mechanisms.

Building upon this analysis, Gupta *et al.* [158] identify six research gaps: (i) the ability to tackle the majority of attacks; (ii) the trade-off between security and performance; (iii) the lack of authenticated cryptography; (iv) the limited focus on deep learning-inspired image cryptographic techniques; (v) the lack of analysis of reconstruction properties during encryption/decryption; and (vi) image cryptography for multispectral imaging. For each identified gap, the authors provide recommendations for future research. For instance, with respect to the first gap, the authors suggest exploring new mechanisms to design robust image ciphers capable of addressing all potential image-related attacks. Such robust ciphers may also help optimize the use of multiple cryptographic algorithms while ensuring high performance and addressing both communication and confidentiality challenges.

Zhang *et al.* [159] present a comprehensive review of the fundamental concepts of chaos and their applications in image information security, including encryption, watermarking, and steganography. The paper begins by introducing the main categories of discrete chaotic maps, such as Logistic, Tent, and Hénon; continuous chaotic systems, including Lorenz, Chen, and Chua; coupled maps, such as *Coupled-Map*

Lattice (CML), *One-Way Coupled-Map Lattice* (OCML), *Global Nonlocal Collapsible Mapping Lattice* (GNCML), *Multiple Dynamic Coupled-Map Lattice* (MDCML), *Improved Sinusoidal Dynamic Non-Adjacent Coupled-Map Lattice* (ISDNCML), and *Non-Adjacent Coupled Dynamic Parameter Mapping Lattice* (NCMLP); memristor-based chaotic systems; general properties of chaos; performance evaluation criteria; and methods for leveraging chaotic dynamics.

Building upon this foundation, Zhang *et al.* [159] discuss chaos-based image cryptography methods in detail, covering spatial-domain techniques, such as scrambling, diffusion, encoding, and substitution, and frequency-domain techniques, including *Discrete Fourier Transform* (DFT), DCT, DWT, and *Fractional Fourier Transform* (FrFT). The authors also review recent studies on watermarking (robust, fragile, and reversible) and steganography (adaptive and static). To outline future research directions, the paper highlights emerging topics such as FPGA-based implementations, quantum encryption, attack resistance and image recovery, as well as deep learning and neural network methods. The review concludes by emphasizing the importance of multidisciplinary integration strategies to enhance both the security and efficiency of chaos-based image information security systems. However, the survey focuses primarily on qualitative discussion, without extensive tabular comparison or quantitative benchmarking.

Jadoon *et al.* [160] present a survey of image encryption schemes, focusing on five taxonomic dimensions: Arnold transformation, chaos-based methods, bit-plane extraction, quantum techniques, and permutation-based algorithms. The study is the first to focus on *Unmanned Aerial Vehicles* (UAVs) operating over insecure communication channels. To enable a consistent comparison, the authors implement and evaluate selected encryption algorithms using *MATrix LABoratory* (MATLAB) 2015 and standard benchmark images, while incorporating previously reported statistical results when available in the surveyed articles. The comparative analysis considers key performance metrics such as information entropy, correlation coefficients, NPCR, UACI, and keyspace. Regarding the proposed taxonomy, chaos-based encryption constitutes the category with eleven studies, the largest number compared to the remaining four taxonomy categories, which collectively account for 21 papers. Among the 32 primary studies surveyed, the authors selected the 21 contributions

most relevant to UAVs applications.

Building upon this analysis, Jadoon *et al.* [160] identify five research challenges, including the trade-off between security and computational efficiency. They also discuss six limitations of the review, such as the lack of attack-surface experimentation, and conclude the survey by outlining five future research directions: UAVs and parallelization with hardware acceleration, machine learning-based security, post-quantum image encryption, blockchain-based key management, and hybrid encryption schemes.

Table 3.1: Selected literature reviews in the SoS

ID	Publication Title	Area	Publisher	Review	Ref	Time	Pg	Cit	Gap	Fut	Score
2013 Sadkhan [140] Iraq	Chaos based cryptography for voice encryption in wireless communication	Voice Encryption	IEEE	Narrative	58	2001 to 2010	8	6	No	Yes	2
2013 Hussain [141] Pakistan	Literature survey on nonlinear components and chaotic nonlinear components of block ciphers	S-Box in Block Ciphers	Springer	Tutorial	73	2005 to 2011	36	17	No	No	2
2014 Zhen [142] China	A Survey of Chaos-Based Cryptography	None	IEEE	Narrative	79	1990 to 2014	8	10	No	Yes	2
2015 Shukla [143] India	Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems	Wired and Wireless Networks	MDPI	Survey	62	1993 to 2015	23	20	No	No	1
2016 Fang [144] China	A Survey on DCSK-Based Communication Systems and Their Application to UWB Scenarios	UWB Wireless Networks	IEEE	SOTA	176	1996 to 2015	34	46	No	Yes	4

Continued on next page

٧٢

ID	Publication Title	Area	Publisher	Review	Ref	Time	Pg	Cit	Gap	Fut	Score
2021 Muthu [145] India	Review of Chaos Detection Techniques in Image Encryption	Chaos Detection	Springer	Survey	99	2007 to 2020	24	8	Yes	No	5
2021 Khaleel [146] Iraq	Chaotic Image Cryptography Systems: A Review	Image Encryption	Other	Survey	49	2010 to 2020	14	3	No	Yes	2
2022 Haseeb [147] Iraq	A Survey on Speech Encryption Using Chaos Map	Voice Encryption	IEEE	Narrative	41	2018 to 2022	6	0	No	No	1
2022 Fang [148] China	A survey of image encryption algorithms based on chaotic system	Image Encryption	Springer	Survey	130	2010 to 2022	29	23	Yes	Yes	4
2022 Zia [149] UK	Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains	Image Encryption	Springer	Survey	165	2016 to 2021	19	53	Yes	Yes	4

Continued on next page

Table 3.1 – continued from previous page

ID	Publication Title	Area	Publisher	Review	Ref	Time	Pg	Cit	Gap	Fut	Score
2022 Zolfaghari [150] Japan	Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap	Image Encryption	MDPI	Survey	279	2014 to 2022	38	25	No	Yes	5
2022 Alhazaimeh [151] Jordan	Chaotic based multimedia encryption: a survey for network and internet security	Multimedia Encryption	Other	Narrative	31	2001 to 2022	9	8	No	No	2
2022 Shraida [152] Iraq	Chaotic-Based Color Image Encryption Algorithms: A Review	Color Image Encryption	Other	Survey	37	2017 to 2022	10	0	No	No	3
2023 Zhang [156] China	Chaos-Based Image Encryption: Review, Application, and Challenges	Image Encryption	MDPI	Survey	204	1996 to 2023	39	35	Yes	Yes	5
2024 Singh [157] India	A systematic literature review on chaotic maps-based image security techniques	Image Encryption	Elsevier	SLR	73	2006 to 2019	11	0	No	No	3
2025 Gupta [158] India	A survey on image cryptography mechanisms: hitherto, and future directions	Image Encryption	Elsevier	SOTA	134	2003 to 2025	24	0	Yes	Yes	5

Continued on next page

Table 3.1 – continued from previous page

ID	Publication Title	Area	Publisher	Review	Ref	Time	Pg	Cit	Gap	Fut	Score
2025 Zhang [159] China	Chaotic Image Security Techniques and Developments: A Review	Image Encryption	MDPI	Survey	171	1997 to 2025	28	0	No	No	4
2026 Jadoon [160] Australia	A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms	Image Encryption	Springer	Survey	214	2017 to 2024	41	0	Yes	Yes	3
2025 Dutra [161] Brazil	A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems	S-Box Block Ciphers	IEEE	SLR	170	1998 to 2025	30	0	Yes	Yes	5

NOTES — ID: Identification, including year of publication, first author, and country. Area: Main area of the work described in the paper. Review type: SLR, addressing specific research questions; *Systematic Mapping Study* (SMS), maps broad research areas and identifies gaps; Survey, collects primary data, generating original quantitative or qualitative insights; Tutorial Review, explains concepts and techniques step-by-step; SOTA, summarizes the most recent advances and trends; Narrative Review, descriptive overview based on the author’s judgment; and Not-a-Review (NoR), primary research, or case studies. Ref: Number of References. Pg: Number of pages. Cit: Number of citations according to <https://scite.ai/>. Gap (Yes or No): Describes research gaps? Fut (Yes or No): Recommends future work? Score (1 to 5): Paper score, 5 being the best.

3.2.3 Synthesis and Analysis

The surveys summarized in Table 3.1 exhibit varying levels of comprehensiveness and quality. Among them, [145, 150, 156, 158] stand out as the most complete and well-prepared, particularly in terms of textual clarity, tables, figures, and comparative analysis, whereas [143, 147] are the least comprehensive. In terms of temporal scope, the surveys cover studies from the early 1990s to recent years.

The geographical distribution reveals a strong concentration in Asia, with 89% originating from China, India, and Iraq. China is the most represented country, contributing five studies, followed by India and Iraq with four articles each. The UK, Japan, Jordan, and Australia each contribute a single article, demonstrating a relatively low diversity of research outside of Asia. Notably, there is an absence of studies from Latin America, Africa, North America, and continental Europe.

The majority of the reviewed papers focus on image and multimedia encryption, which constitutes approximately 61% of the total studies analyzed. As reported in [148–152, 156], chaos-based cryptography approaches are particularly suitable for this application, as image encryption demands both diffusion and confusion mechanisms to effectively scramble pixel positions and alter pixel values—properties inherently provided by chaotic systems. In addition to image encryption, other areas of focus include voice encryption (11%), with smaller contributions from areas such as wireless networks and cryptographic primitives. This distribution highlights the prominence of image encryption in the chaos-based cryptography landscape while also reflecting the broader applicability of chaotic systems to various cryptographic tasks, including voice and multimedia encryption, where similar principles of diffusion and confusion are equally critical.

The taxonomy employed by the surveys listed in Table 3.1 for categorizing the reviewed papers and structuring the corresponding discussion is highly heterogeneous, reflecting the diversity of approaches within the field of chaos-based cryptography. Several surveys adopt a temporal classification, grouping papers according to their year of publication. In these cases, older studies are often summarized collectively in a single paragraph with limited analysis, while more recent papers are examined in greater detail. Other surveys implement a taxonomy based on the intrinsic characteristics of the chaotic maps and systems utilized in the reviewed

studies, considering parameters such as system dimensionality, the type of system (continuous or discrete), and dynamical indicators like the Lyapunov exponent.

Additional classification schemes focus on cryptographic methods, including symmetric encryption, stream and block ciphers, and asymmetric encryption, exemplified by algorithms such as ECC, RSA, and ECDSA, as well as cryptographic hash functions. Some surveys extend this categorization to hybrid cryptography algorithms, integrating chaos-based cryptographic schemes with complementary techniques such as DNA-based methods, artificial intelligence, neural networks, and blockchain technologies. Other approaches categorize the reviewed studies according to their application domains, encompassing areas like military systems, satellite communications, multimedia processing, and general communication networks. Finally, a subset of surveys organizes the works based on the signal processing domain, distinguishing between time-domain and frequency-domain applications, which is particularly relevant for understanding the operational context and performance of chaos-based cryptographic schemes.

As seen in Table 3.1, the listed reviews can be classified into seven types: SLR, SMS, Survey, Tutorial, SOTA, Narrative, and *Not a Review* (NoR). Only the study by Singh [157] reaches the most comprehensive level of an SLR in the field of chaos-based cryptography. Most of the listed works are narratives (22%) or surveys (56%), focusing on selected aspects of the field, such as particular chaotic maps, cryptographic techniques, or specific application domains, rather than adhering to a structured review process that meets established standards. Consequently, while these surveys provide valuable insights, they often lack the methodological rigor and transparency expected from a formal SLR.

A deeper analysis is necessary to understand the reasons why only one review of type SLR appears in Table 3.1. Firstly, this scarcity can be attributed to the relative immaturity of the field. Most research on chaos-based cryptography has emerged from applied domains, where the focus has been on practical implementation results rather than formal review processes. As a result, many studies have been conducted by authors with limited attention to methodological rigor. Secondly, the absence of methodological standardization has exacerbated this limitation. Unlike the health sciences, where SLR frameworks have become widely established, cryp-

tography has not traditionally adopted formalized guidelines for conducting SLRs. This explains the prevalence of descriptive and narrative surveys in Table 3.1, rather than systematic ones. Thirdly, the inherently interdisciplinary nature of chaos-based cryptography has led to methodological fragmentation. Research in this field spans multiple communities, including mathematics, electrical engineering, computer science, and applied cryptography, each employing distinct analytical frameworks. Finally, the pressure for rapid publication has contributed to the production of concise surveys that prioritize speed over methodological rigor, often lacking reproducible search strategies, transparent inclusion and exclusion criteria, or systematic data extraction and quality assessment procedures.

This context reinforces the rationale for structuring the present work as a formal SLR. Beyond addressing a research gap in the literature — specifically, the absence of any prior SLR in chaos-based cryptography focused on S-Boxes — this study represents the first SLR in this domain and also addresses a long-standing methodological deficiency in the field. By adopting an established systematic review framework, such as PRISMA, and the guidelines proposed in [138,139], this work not only consolidates dispersed research findings but also enhances the methodological rigor of chaos-based cryptography research. In doing so, it bridges the gap between applied cryptographic experimentation and formal evidence synthesis, establishing this review as both a scientific contribution and a methodological benchmark for future studies in the field.

3.3 Systematic Literature Review: New Frontiers

This section defines the scope and positioning of this SLR, as well as its main contributions and the methodology adopted throughout the remainder of this work, based on the analysis of Table 3.1 and the discussions presented in Sections 3.2.2 and 3.2.3. The scope of this study is to systematically review, evaluate, and synthesize the literature on chaos-based cryptography, with particular emphasis on the use of S-Box.

The positioning of this SLR is motivated by gaps identified in the survey of surveys (SoS) summarized in Table 3.1. Specifically, most existing reviews focus on

isolated aspects, such as particular chaotic maps, encryption techniques, or application domains; only one study [157] follows formal SLR guidelines; and none conducts a systematic review specifically addressing S-Boxes within the context of chaos-based cryptography. Consequently, the proposed SLR constitutes a novel contribution to this field.

The contributions of this work are threefold: (i) a systematic survey of primary studies on chaos-based cryptography utilizing S-Boxes; (ii) a structured classification of the surveyed primary studies; and (iii) the identification of research gaps, along with recommendations for future work. This SLR is reported as the final entry in Table 3.1 and is further summarized in Table 3.2 for ease of reference.

Table 3.2: Positioning of this SLR within chaos-based cryptography surveys

ID	Title	Area	Publisher	Review	Ref	Time	Pg	Cit	Gap	Fut	Score
2025 Dutra [161] Brazil	A Systematic Literature Review										
	on the Application of Chaos	S-Box				1998					
	Theory to the Design of	Block	IEEE	SLR	170	to	30	0	Yes	Yes	5
	Substitution Boxes for	Ciphers				2025					
	Cryptographic Systems										

NOTES — ID: Identification, including year of publication, first author, and country. Area: Main area of the work described in the paper. Review type: SLR, addressing specific research questions; SMS, maps broad research areas and identifies gaps; Survey, collects primary data, generating original quantitative or qualitative insights; Tutorial Review, explains concepts and techniques step-by-step; SOTA, summarizes the most recent advances and trends; Narrative Review, descriptive overview based on the author’s judgment; and Not-a-Review (NoR), primary research, or case studies. Ref: Number of References. Pg: Number of pages. Cit: Number of citations according to <https://scite.ai/>. Gap (Yes or No): Describes research gaps? Fut (Yes or No): Recommends future work? Score (1 to 5): Paper score, 5 being the best.

3.3.1 Methodology

The objective of this study is to conduct a SLR on the application of chaos theory to encryption algorithms, with a particular focus on the design of S-Boxes as sources of confusion, while also examining the broader use of chaotic systems in cryptographic primitives.

Within the research protocol, the PICOC criteria are defined as follows: Population: cryptographic algorithms, with an emphasis on S-Boxes; Intervention: the application of chaos theory to the design of S-Boxes; Comparison: not applicable; Outcome: the evaluation of core cryptographic properties; and Context: peer-reviewed academic studies in the field of chaos-based cryptography.

Given their central role in structuring the analysis and ensuring methodological rigor, the following research questions are formulated to achieve the objectives of this study and guide the systematic review process:

- (1) What implementation approaches (software, FPGA, ASIC) have been adopted for chaos-based cryptography employing S-Boxes?
- (2) How has the number of publications on chaos-based cryptography using S-Boxes evolved over the years?
- (3) How many studies on S-Boxes within chaos-based cryptography have been published by each publisher?
- (4) What are the bibliometric characteristics of the studies, including the number of pages, citations, references, and age since publication?
- (5) Are the chaotic outputs precomputed or generated OtF in each study?
- (6) Is the keyspace (K_s) computed based on the characteristics of the chaotic system or map in each study?
- (7) Is the transient time considered in each study, and is it derived from the chaotic properties of the chosen system or map?

The following digital libraries were considered in this SLR: ACM Digital Library, Google Scholar, IEEE Xplore, MDPI, ScienceDirect (Elsevier), SpringerLink,

and Wiley. The search strategy assessed whether each primary study lies at the intersection of three concepts: (i) encryption (search terms: cryptographic, cryptography, cryptanalysis, encryption, decryption, algorithm, block, cipher, stream, symmetric); (ii) chaos (search terms: chaos, chaotic, dynamics, generator, map, non-linear, pseudo-random, sequence, system, theory); and (iii) substitution box (search terms: box, S-Box, confusion, diffusion, LUT, lookup table, primitive, substitution, permutation).

The selection criteria begin by checking for the presence of the three aforementioned concepts in the title, keywords, and abstract fields. The quality assessment checklist consists of seven questions:

- (1) Is the research objective or problem clearly stated in the abstract?
- (2) Does the abstract highlight the contribution of the study (e.g., a new method, evaluation, or comparison)?
- (3) Does the abstract mention the use of chaotic systems or maps in cryptography?
- (4) Is the cryptographic primitive or scheme (e.g., S-Box, PRNG, cipher) specified in the abstract?
- (5) Are performance or security aspects addressed in the abstract (e.g., efficiency, strength, robustness)?
- (6) Does the study combine chaos with other techniques (e.g., artificial intelligence, DNA computing)?
- (7) Was the study published in a peer-reviewed journal of recognized quality?

An affirmative answer to each question receives one point, a negative answer receives zero points, and a partial answer receives 0.5 points. Consequently, the maximum possible score is seven points for studies that meet all criteria. A cutoff score of 4.5 points was defined; studies scoring below this threshold were excluded from subsequent data extraction.

The data extraction form is designed to systematically collect the following categories of information:

- (i) Bibliographic identification: year, first author, BibTeX reference, country, journal or conference, and publisher;
- (ii) Bibliometric information: number of pages, number of references cited, total citations, citing and cited publications, age of publication in years, reviewer quality score, and final grade;
- (iii) Chaotic system details: dimension, keyspace, transient time, on-the-fly chaos computation during encryption, and potential chaos degradation issues (Yes/No);
- (iv) Cryptographic primitives studied: S-Box, PRNG, block cipher, stream cipher, hash, ECC; S-Box description, chaotic system, and hybrid technologies (DNA, AI, ML, blockchain, genetic algorithms);
- (v) Application domains: military, satellite, medical, IoT, cloud, network security, multimedia, image, text, general-purpose, or other;
- (vi) Implementation platforms: FPGA, ASIC, CPU, software, MATLAB, Python, C/C++, or other environments;
- (vii) S-Box evaluation techniques: cryptographic metrics (nonlinearity, bijectivity, SAC, BIC, etc.) and security metrics (resistance to linear and differential attacks, etc.);
- (viii) Cipher evaluation techniques: statistical visualization (e.g., histogram), statistical tests (e.g., chi-square, correlation, entropy, NIST/Diehard), and performance metrics (throughput, latency, memory usage, hardware resources, etc.).

This SLR reviews primary studies published between 2001 and 2026 in the field of chaos-based cryptography. The analysis is organized into three complementary perspectives. First, Design Considerations examines the practical and theoretical requirements for the secure use of chaotic systems in cryptography, including the selection of valid initial conditions, attractor dynamics, ergodicity, implementation efficiency, and the effects of chaos degradation in digital realizations. Second, Pioneering and Influential Studies investigates the seminal contributions that established and shaped the development of the field. Third, State-of-the-Art analyzes

recent advances, hybrid approaches, and emerging research directions. The resulting synthesis provides a structured overview of the literature, identifies research gaps, and highlights opportunities for future work.

A total of 688 publications were imported into the Parsifal tool, all of which were subjected to title and abstract screening based on predefined inclusion and exclusion criteria. After this screening phase, 216 studies were retained. Subsequently, a quality assessment was conducted, in which the studies were scored according to seven criteria related to clarity of objectives, stated contributions, use of chaos in cryptography, identification of cryptographic primitives, discussion of security/performance aspects, combination with other techniques, and publication in peer-reviewed journals. Based on a threshold score, 28 studies were selected for full-text analysis and 26 for data extraction. The overall selection process is quantitatively illustrated in the PRISMA diagram shown in Figure 3.2.

3.3.2 Data Extration

Chaos and cryptography are intimately tied, as the fundamental cryptographic properties of confusion and diffusion are closely associated with the chaotic characteristics of ergodicity and sensitivity to initial conditions, as discussed in Section 2.2.2. This relationship has led many researchers to develop chaos-based cryptographic algorithms and to explore both the theoretical foundations and practical constraints of using chaotic systems in encryption, as will be examined in this Section 3.3.2.

3.3.2.1 Design Considerations

When applying chaos theory to cryptography, several critical and performance-related aspects must be considered; otherwise, the cipher may exhibit exploitable weaknesses.

The paper "Advantages of the Linz-Sprott weak nonlinearity on the FPGA implementation of chaotic systems: a comparative analysis" [162] discusses key aspects of FPGA implementation of chaos-based cryptographic systems. A fundamental property of chaotic systems is their NL, typically expressed as the multiplication

of variables, as in the terms xz and xy in the Lorenz chaotic system. The study highlights the hardware advantages of using the modulo operation $|x|$, as proposed by Linz and Sprott [11], which requires only a sign-bit change.

The paper "Chaotic Equations Initial Conditions Analysis for Cryptography Applications" [2] demonstrates that only specific ICs lead a chaotic map or system to exhibit a strange attractor, which is a critical property for encryption algorithms due to their sensitivity to initial conditions and ergodicity. Otherwise, inappropriate ICs may cause the system to converge or diverge, thereby making the cipher predictable and vulnerable. This concept was further extended in [4] to propose a novel method for implementing encryption algorithms based on chaotic systems. The method considers not only the attractor basin but also its ergodicity, the number of encryption keys associated with the volume of valid ICs, and the time response.

Acikkapi *et al.* [163] introduce a systematic method to determine the most suitable ICs for chaotic maps for statistical randomness applications. It combines theoretical analysis with randomness test suites to identify ICs that maximize unpredictability while avoiding convergence to periodic or degenerate behavior. The approach ensures that the selected ICs yield sequences with strong statistical properties, thereby enhancing the reliability of chaos-based cryptographic primitives.

Wen *et al.* [164] discuss chaos degradation [165] as a critical issue for the practical deployment of chaotic systems in secure communications and cryptography. Their analysis shows that, due to numerical errors, finite precision in digital implementations, and hardware limitations, the inherent chaotic dynamics may deteriorate into periodic or quasi-periodic behavior, significantly reducing unpredictability. This phenomenon directly impacts the effectiveness of chaos-based cryptography, as it compromises sensitivity to initial conditions and ergodicity, two essential properties for ensuring strong security. Chaos degradation is further discussed in [166], showing that the loss of true chaotic characteristics can introduce vulnerabilities to cryptanalysis and highlights the necessity of designing degradation-resistant chaotic models.

3.3.2.2 Pioneering and Influential Studies

Since the seminal study of Matthews [167] in 1989, numerous studies have been published in the field of chaos-based cryptography [18–21, 23, 25–28, 30–36, 39, 41, 49, 51, 54, 55, 58–61, 127–137].

Gotz *et al.* [19] propose a systematic design for discrete-time coders, in which encryption arises from inherent chaotic behavior. The design approach in [19] is implemented in [18] and subsequently cryptanalyzed in [20] through two different ciphertext-only attacks, leading to proposed improvements to the coder system. Baptista [21] encrypts each character of a text message as the number of iterations performed in the logistic chaotic map, to transfer the trajectory from an initial condition to a portion of the logistic chaotic attractor related to the ciphertext. Alvarez *et al.* [23] describe a computational procedure to encrypt a message, provided that the transmitter and receiver have access to identical but non-synchronized chaotic dynamical systems. The technique is based on the fact that the symbolic dynamics of these systems can be used to sequentially construct data blocks that reproduce those of the input file.

The paper "From Chaotic Maps to Encryption Schemes" [22] explores the application of chaotic maps for the design of encryption schemes. The paper establishes a theoretical framework for understanding chaos and its mathematical foundations, with a focus on discrete chaotic maps. These systems are analyzed for their ability to generate pseudorandom sequences by partitioning the state space into a finite number of regions. The paper emphasizes the need for rigorous evaluation of chaotic systems to ensure they satisfy essential cryptographic criteria, including randomness, NL, and resistance to cryptanalytic attacks.

The paper [22] further explains how chaotic systems can be analyzed using symbolic dynamics, a process in which the state space is partitioned into regions, symbols are assigned to these regions, and the resulting macroscopic behavior is observed. Although initially deterministic, such systems exhibit an apparent loss of determinism, as different initial conditions within the same region evolve unpredictably over time, thereby requiring probabilistic descriptions. This partitioning transforms the system into an ergodic information source, in which the long-term behavior becomes independent of initial conditions for mixing maps. The paper also

discusses the synchronization of two chaotic systems for secure information transmission, leveraging this phenomenon to encode and decode messages. Although it does not address cryptanalysis, it analyzes and plots four statistical measures as functions of the number of iterations: (i) the average number of 1s in a ciphertext block when the plaintext contains a single bit set to 1; (ii) the average number of differing bit positions between two ciphertext blocks when the corresponding plaintext blocks differ in only one bit; (iii) the average number of differing bit positions between two ciphertext blocks when the plaintext is all zeros and the corresponding keys differ in only one bit, with one key equal to zero; and (iv) the average number of differing bit positions between two ciphertext blocks when the plaintext is all zeros and the keys differ in only one bit. These results illustrate the strength of the proposed encryption scheme.

The paper "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps" [24] extends the work of [22] and explores the application of discrete chaotic maps to the design of block ciphers. The chaotic properties of sensitivity to initial conditions and ergodicity are closely related to the cryptographic principles of confusion, which decorrelates the plaintext and ciphertext, and diffusion, which spreads information across the ciphertext. The state space of the chaotic system is partitioned into distinct regions, each labeled with a symbol. This partitioning transforms the deterministic chaotic system into a probabilistic model, enabling the use of information theory to analyze its behavior.

The encryption process described in [24] involves iterating the chaotic map and encoding the plaintext through transformations driven by the map output. The algorithm amplifies small differences in the plaintext or key, leading to significant changes in the ciphertext, a property that is critical for resisting cryptanalytic attacks such as differential and linear cryptanalysis. The authors demonstrate the algorithm's diffusion capability, ensuring that minor input changes produce significant output differences. They argue that the inherent unpredictability of chaotic maps provides a rigorous mathematical foundation for secure encryption. The paper presents three chaos-based cryptographic schemes: an algorithm based on the logistic map (2.2), in which the function f is not one-to-one; an algorithm based on an exponential function with a one-to-one f ; and an algorithm based on the n -th

iteration of the logistic map, resulting in a precomputed 256-entry substitution box (S-Box) that forms the basis for a 64-bit Feistel network.

Li *et al.* [25] propose *Chaotic Video Encryption Scheme* (CVES) that employs multiple chaotic maps, a PRNG, and a hybrid combination of stream and block ciphers, achieving fast, secure, and compression-independent real-time video encryption, and is extensible to both hardware and software implementations.

Wong [26] proposes a fast chaotic cryptographic scheme based on an iterated logistic map, which dynamically updates a lookup table without generating random numbers, significantly reducing encryption and decryption time, thereby enabling practical secure transmission of large multimedia files. Subsequently, Wong [28] shows that the final lookup table after encryption depends on the message, serving as a hash function, and generalizes the chaotic scheme in [26] to perform both encryption and hashing, with collision resistance analysis. Later that year, Wong *et al.* [27] observe that reducing iteration counts speeds up encryption, but the ciphertext remains at least twice the original length; they modify the previous scheme [26] to shorten the ciphertext and introduce a session key, resulting in variable ciphertext length.

3.3.2.3 State of the Art

Inspired by the pioneering studies in Section 3.3.2.2, we now turn to the core of this SLR, as outlined in Section 3.3, which aims to systematically review, evaluate, and synthesize the literature on chaos-based cryptography, with emphasis on the use of S-Boxes.

The paper "A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map" [52] presents three main contributions: a novel compound chaotic system derived from a two-dimensional hyper-chaotic map combined with quantum random walks, a dynamic S-Box generation algorithm, and a security analysis comparing the proposed S-Box with five existing S-Boxes. First, Zhang *et al.* [52] introduce and analyze a simplified two-dimensional chaotic map using trajectory plots, Lyapunov exponents, and bifurcation diagrams. Subsequently, a PRNG is designed based on the compound chaotic system, which passes all 17 tests in the NIST SP800-22 suite. A 16×16 S-Box is dynamically

generated using the proposed chaos-based cryptographic algorithm. This S-Box is evaluated in terms of its cryptographic strength using criteria including the strict avalanche criterion, bijection, NL, bit independence, linear approximation probability, and differential probability. Finally, a security analysis is conducted on the proposed S-Box against algebraic, differential, linear, and boomerang attacks. The study does not address the hardware implementation of dynamically key-dependent S-Boxes, focusing instead on the analysis of a single generated S-Box. Although the authors discuss chaos degradation, the study does not provide an in-depth analysis of the topic.

The paper "A Novel Approach for Designing Dynamic S-Boxes Using Hyperchaotic System" [37] presents a novel method for generating dynamic S-Boxes for cryptographic applications. The method employs a four-dimensional hyperchaotic Lorenz system to generate dynamic S-Boxes and enhance the security and robustness of encryption algorithms. The hyperchaotic Lorenz system, characterized by higher dimensionality and greater unpredictability than traditional chaotic systems, incorporates a nonlinear feedback controller u into the second equation of (2.3) and introduces a fourth equation $\dot{u} = -kx$, where k is a constant ranging from 0 to 16.6. This modification results in two positive Lyapunov exponents.

The proposed scheme in [37] exploits the sensitivity to ICs and control parameters inherent in hyperchaotic systems to generate key-dependent S-Boxes, thereby enhancing their resistance to cryptanalysis. The core idea consists of initializing and evolving a hyperchaotic Lorenz system using a set of initial conditions to produce a chaotic sequence, which is subsequently used to generate a set of 500 S-Boxes through a four-step algorithm. This algorithm is defined over the parameter set $(x_0, y_0, z_0, u_0, k, N)$, where $k \in [0, 16.6]$ and N denotes the number of iterations. The cryptographic strength of the generated S-Boxes is evaluated using standard cryptographic criteria, including bijectivity, NL, DAP, standard deviation, histogram analysis, correlation, SAC, and BIC. The generated S-Boxes are further compared with benchmark S-Boxes reported in [24, 29, 168]. The dynamic nature of the S-Boxes generation scheme enables periodic regeneration, thereby introducing an additional layer of security by mitigating vulnerabilities associated with static cryptographic structures. The authors highlight the potential applications of the proposed approach in

secure communication, digital watermarking, and hardware-based cryptography.

The paper "A Novel Design of Chaos-Based S-Boxes Using Genetic Algorithm Techniques" [38] proposes a hybrid approach for constructing S-Boxes by combining chaotic maps with genetic algorithms. The method exploits the intrinsic chaotic properties, such as sensitivity to initial conditions, to generate an initial population of S-Boxes. The chaotic Logistic Map (2.2), with control parameter $R = 3.99999$, is employed to generate the initial S-Box, while the chaotic Lorenz system (2.3), with parameters $a = 10$, $b = 28$, and $c = 8/3$, is used to control the crossover (row and column shuffling) and mutation (value permutation) operations of the genetic algorithm. The initial S-Box and all generated offspring are bijective, as duplicate values are eliminated during the population generation process.

In [38], the Logistic and Lorenz chaotic maps are iterated 100 times before generating the output sequences, without a thorough analysis of whether this number is sufficient to mitigate transient chaotic dynamics. This pitfall is present in many studies and will be analyzed in greater depth in Section 3.3.3. More than 10^5 S-Boxes were generated, from which the seven best-performing candidates (with nonlinearity ≥ 107) were selected. The performance of these seven S-Boxes was evaluated in terms of their average nonlinearity and average SAC. The generated S-Boxes were further compared with four S-Boxes reported in the literature with respect to four properties: NL, SAC, BIC, and equiprobable input/output XOR distribution.

Tang and Liao [29] present an approach for constructing dynamic S-Boxes for cryptographic applications based on discretized chaotic maps. Static (or fixed) S-Boxes are time-invariant and are typically predefined prior to encryption, remaining unchanged during operation and independent of the secret key. As a result, they are more susceptible to cryptanalytic attacks once their structure becomes known. The method proposed in [29] introduces dynamic behavior by employing discretized chaotic maps, with emphasis on the skew tent map, to generate S-Boxes that evolve during the cryptographic process. The framework incorporates a discretization process to address the incompatibility of continuous chaotic systems with digital computation, thereby enabling practical implementation.

A total of 120 S-Boxes generated in [29] are reported to exhibit desirable

cryptographic characteristics based on five criteria: bijectivity, NL, SAC, BIC, and equiprobable input/output XOR distribution. The proposed method consists of three steps: first, an integer sequence, regarded as a secret key K , is selected; second, the skew tent chaotic map is iterated more than $k = 39$ times from the initial value X_0 to obtain a final value X , although the choice of the minimal iteration count $k = 39$ is not thoroughly justified; third, the resulting value X is mapped into a $2^{n/2} \times 2^{n/2}$ table, yielding the desired S-Box. The designed S-Box is compared with that proposed in [169] using the same evaluation criteria and demonstrates superior statistical performance. Tang's approach [29] also briefly addresses key sensitivity and resistance to prediction by incorporating key-dependent parameters, such as the number of iterations k and the constant A of the skew tent map, suggesting future enhancements for improved security.

The paper "A New 12-Bit Chaotic Image Encryption Scheme Using a 12×12 Dynamic S-Box" [57] proposes an encryption method optimized for 12-bit grayscale medical images. Conventional 8-bit encryption schemes may be inadequate for such data because they either truncate valuable information or require multiple operations, thereby reducing efficiency. The authors present a scheme that employs a key-dependent 12×12 dynamic S-Box combined with a chaotic Baker map for diffusion. The encryption process involves two rounds of S-Box substitutions and XOR masking using flipped chaotic sequences, followed by a final substitution step. The key-dependent S-Box construction algorithm is adapted from [170] and combines two components: the Mersenne Twister PRNG and the Fisher-Yates shuffle.

In [57], the performance evaluation includes entropy, histogram analysis, cross-correlation, spatial autocorrelation, NPCR, UACI, key sensitivity, resistance to CPA, keyspace evaluation, and encryption speed measured on a Java Virtual Machine (JVM) version 1.8 running on an Intel Core i7-8565U processor at 1.8 GHz with 12 GB of *Random Access Memory* (RAM). The proposed scheme achieves throughput up to 300 MB/s, approximately three times faster than comparable 8-bit systems. The authors justify the design by analyzing the effects of the number of rounds, mask flipping, the final substitution, and the impact of using a 12×12 S-Box instead of an 8×8 one. Finally, the security and efficiency of the proposed method are compared against more than ten similar works using metrics such as

entropy, correlation analysis, NPCR, UACI, key sensitivity, and encryption time.

The paper "An Image Encryption Algorithm Based on the Chaotic Lorenz System and Novel Primitive Polynomial S-Boxes" [47] presents an encryption method that combines the unpredictability of chaotic systems with mathematically constructed polynomial S-Boxes. This work introduces 16 distinct S-Boxes derived from a projective general linear group in combination with 16 primitive irreducible polynomials defined over the Galois field of order 256, exhibiting strong algebraic properties, including high NL and bijectivity. The encryption algorithm comprises three stages: chaotic permutation, S-Box-based substitution, and dynamic diffusion.

In [47], the chaotic Lorenz system generates sequences for pixel-level scrambling in the permutation phase, disrupting the intrinsic spatial correlation of images. The substitution stage employing the S-Box introduces NL and enhances cryptographic robustness, while the dynamic diffusion stage alters pixel values based on chaotic sequences and dependencies between neighboring pixels, ensuring that even minor changes in plaintext result in significant modifications in the ciphertext. The performance evaluation includes histogram analysis to confirm uniform pixel intensity distribution in the ciphertext, key sensitivity tests, entropy analysis, and adjacent pixel correlation analysis. These results demonstrate the effective elimination of correlations present in plaintext images. Furthermore, resistance to differential attacks is verified using NPCR and UACI metrics. Computational efficiency tests demonstrate the algorithm's suitability for real-time encryption applications. The proposed method is compared against four encryption schemes reported in the literature.

A drawback of the work in [47] is the decision to discard the first 100 values generated by the chaotic Lorenz system to improve randomness, without a thorough analysis of whether this number of iterations is sufficient to mitigate transient effects. Another weakness lies in treating the parameters $a = 10$, $b = 28$, and $c = 8/3$ as initial conditions of the Lorenz chaotic system and relating them to the keyspace. In fact, deviating these parameters from their well-established values in the literature may drive the system into a non-chaotic regime, thereby compromising the cryptographic properties derived from chaotic behavior.

The paper "Bijective S-Boxes Method Using Improved Chaotic Map-Based

Heuristic Search and Algebraic Group Structures" [43] proposes a method for generating cryptographically secure S-Boxes that combines chaotic systems and algebraic group structures. The authors introduce an improved one-dimensional chaotic map that exhibits enhanced chaotic properties compared to existing maps, such as the logistic map, logistic-sine system, and one-dimensional sine-powered map. This map is characterized by a larger Lyapunov exponent, higher entropy, and a wider range of the control parameter r that yields chaotic behavior. The proposed hybrid S-Box construction method is divided into two parts: (1) chaotic heuristic search and (2) algebraic group structures and actions.

The first part of [43] consists of nine steps, beginning with the definition of the input parameters: $X_0 = 0.234$, the initial state of the proposed 1-D chaotic map; $\Delta = 250$, the number of iterations of the chaotic map; $N = 1000$, the number of generations; and $n \in [5, 8]$, the size of the generated S-Box. The chaotic map parameter is set to $r = 3.9$. Step 5 of the algorithm guarantees bijectivity, as a value w , computed from the current state X , is assigned to a given S-Box (S_1 , S_2 , or S_3) only if it has not been previously assigned. A potential weakness of the algorithm lies in the use of the Δ parameter (the number of cycles the chaotic map is iterated) without considering an adequate decorrelation time for the final states of the chaotic map.

The second phase of the proposed hybrid method in [43] focuses on enhancing the cryptographic properties of the S-Boxes (S_1 , S_2 , or S_3) generated in the previous stage using algebraic group-based transformations. This process involves determining suitable groups whose actions enhance the cryptographic strength of each S-Box. The group selection procedure is performed individually for each S-Box. The security performance of the generated S-Boxes is analyzed using the following criteria: NL, a key metric for resistance to linear cryptanalysis; SAC, which measures the probability (ideally 0.5) of output bit changes when a single input bit is flipped; BIC-SAC and BIC-NL; DAP, indicating resistance to differential cryptanalysis; and LAP, which measures input-output bit distribution uniformity, where lower values imply stronger resistance against linear attacks. The proposed S-Boxes are compared with more than twenty-five S-Boxes reported in the literature using these metrics and are reported to achieve competitive results.

In [43], an S-Box of dimension 8×8 generated by the proposed method was applied to encrypt the standard 8-bit grayscale Lena image of size 256×256 using a bidirectional S-Box-based substitution process: first, the S-Box substitutes the plaintext pixels in a forward direction from the first to the last pixel, and then the same S-Box is applied in reverse on the resulting ciphertext from the last to the first pixel. The encryption performance was evaluated using the MLC and standard statistical measures, including entropy, correlation, contrast, energy, and homogeneity.

The paper "A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes" [50] presents a color image encryption scheme that integrates hyperchaotic systems and DNA genetic codes. The proposed method utilizes a 4-D hyperchaotic system (with two multiplicative nonlinearities and two positive Lyapunov exponents) alongside a 1-D chaotic logistic map. Hyperchaotic systems, due to their higher-dimensional complexity, provide enhanced randomness, as they are highly sensitive to initial conditions and parameters, making them well-suited for cryptographic applications.

In [50], the method is described as follows: a chaotic intermediate image (I^c) is generated using a logistic map to produce a key k_o . The size of (I^c) is set equal to that of the plaintext image (I^p). By hashing (I^c) using a SHA algorithm of type 2 with 512-bit output, another key k_1 is generated. The keys k_o and k_1 are concatenated and processed through SHA-512 to obtain the final key k_I . Then, the initial conditions and seeds for the 4-D hyperchaotic system are derived from k_I . Subsequently, *Red-Green-Blue* (RGB) S-Boxes based on this 4-D hyperchaotic system are constructed.

The paper [50] then decomposes (I^p) and (I^c) into n sub-blocks, which are processed through a DNA encoder, followed by DNA operations, a DNA decoder, and a reshaping unit to produce the first-stage encrypted image. The DNA encoding and operations are guided by values generated from the logistic map. Finally, substitution is performed using the RGB S-Boxes to generate the final ciphertext image. Decryption follows the inverse of these steps, executed in reverse order from bottom to top.

The study in [50] presents a comprehensive performance and security evalu-

ation using MATLAB R2015a. This includes image encryption quality analysis of four color images based on PSNR; NIST SP800-22 randomness tests, all of which were successfully passed; keyspace analysis showing up to 2^{428} possible keys, well above the commonly accepted security threshold of 2^{100} for resistance to BFA; and key sensitivity tests demonstrating decryption failure under slight key variations, illustrated using a pediatric COVID-19 pneumonia image with SHA hashing and average NPCR.

Further analysis in [50] includes differential analysis using NPCR and UACI; correlation analysis of 5000 adjacent pixel pairs, where values are close to 1 for plaintext images and close to 0 for encrypted images; histogram uniformity evaluation using Pearson's chi-square test (χ^2); texture features derived from *Gray Level Co-occurrence Matrix* (GLCM), including contrast (Cn), energy (En), and homogeneity (Hm); entropy analysis of encrypted image randomness; and resistance to KPA and CPA attacks simulated using RGB-black and RGB-white images. These tests yielded NPCR values of 99.51% and 99.49%, respectively.

Additionally, *Mean Absolute Error* (MAE) was used in [50] to evaluate the dissimilarity between I^e and I^p , and robustness against noise and occlusion was tested using 5% salt-and-pepper noise, 1% Gaussian noise, speckle noise, and occlusion levels of 12%, 25%, and 50% using black pixels. *Encryption Quality* (EQlty) was used to quantify the total number of pixel changes, and computational complexity was analyzed across all stages, including DNA encoding/decoding, chaotic permutations, S-Box generation, and RGB substitutions. Lastly, encryption efficiency was measured using *Average Encryption Time* (AvgEncT), *Average Decryption Time* (AvgDecT), *Average Encryption Throughput* (AvgEncTh), and *Average Number of CPU Cycles per Byte* (AvgNCPB).

Although the algorithm proposed in [50] demonstrates strong cryptographic performance, it lacks analysis of bijectivity in the proposed S-Boxes. Furthermore, the keyspace analysis considers all combinations of key inputs but does not account for the possibility that certain initial conditions may drive the chaotic map into non-chaotic regimes, thereby compromising the security properties associated with chaotic behavior.

The paper "A New Dynamic Substitution Box for Data Security Using an

Innovative Chaotic Map" [5] introduces a novel S-Box within a chaotic-based cryptographic framework using block ciphers as primitives. It proposes a new 1-D chaotic map, called *Malik, Atif, and Zahid chaotic Map* [5] (MAZa), which combines characteristics of the logistic and sine maps, exhibiting improved bifurcation behavior and higher Lyapunov exponents compared to the original logistic and sine maps. The preliminary S-Box is constructed by directly mapping values $X \in [0, 255]$, generated from the MAZa map, into a 16×16 matrix at positions (i, j) determined by the algorithm. Subsequently, a second heuristic algorithm, guided by key-derived parameters, performs dynamic swapping of (i, j) positions to produce the final key-dependent S-Box.

The security analysis of the method proposed in [5] was conducted using widely accepted cryptographic criteria, including bijectivity, NL (measured via Walsh–Hadamard transform), absence of fixed points in the final S-Box [171], SAC and BIC [172], LAP and DAP, computational efficiency (100,000 S-Boxes were simulated using Visual C#), and keyspace size, estimated at 2^{164} , which is considered sufficient to withstand BFA. The authors identified two limitations in the proposal: the one-dimensional nature of the MAZa chaotic map and the limited comparative analysis, which includes only the logistic and sine maps. A critical drawback, however, is the omission of an analysis of initial conditions that might drive the MAZa map into a non-chaotic regime, potentially compromising the desired unpredictability.

The paper "Advancing Cryptographic Security with a New Delannoy-Derived Chaotic S-Box" [56] introduces a novel approach for constructing secure S-Boxes by combining the mathematical framework of Delannoy numbers with a five-dimensional (x, y, z, w, v) hyperchaotic system. This system comprises eight constant parameters (a, b, c, d, e, f, g, h) , three nonlinear terms (yz, xy, x^2y) , and exhibits three Lyapunov exponents $(L_1 = 9.979, L_2 = 1.96, L_3 = 0.005362)$. The parameters are set to $(10, 60, 20, 15, 40, 1, 50, 10)$, and the initial states $(x_0, y_0, z_0, w_0, v_0)$ are set to $(1, 1, 1, 1, 1)$.

In [56], Delannoy numbers $D(m, n)$ count the number of lattice paths from $(0, 0)$ to (n, m) using only three types of moves: right $(1, 0)$, up $(0, 1)$, and diagonal $(1, 1)$. The proposed method consists of a sub-algorithm named *Delannoy Number*

Generator, which computes the Delannoy numbers $D(m, n)$. These values are then used by the main algorithm, *DNB SBox*, to construct the final S-Box. A 16×16 S-Box is generated and evaluated using standard criteria: bijectivity, NL, SAC, BIC, LAP, and DAP. Furthermore, the proposed S-Box is compared with ten existing S-Boxes from the literature, demonstrating superior performance according to the reported metrics.

Although designed for symmetric key cryptography, the authors of [56] suggest potential applicability in other cryptographic primitives such as message authentication codes, hash functions, digital signatures, stream ciphers [53], password-based encryption, disk encryption, and secure communication protocols. The authors acknowledge that using a five-dimensional hyperchaotic map introduces significant computational overhead, which could be mitigated in future work by adopting a lower-dimensional chaotic map. Additionally, the paper lacks a thorough investigation of the initial conditions that lead to chaotic behavior. Selecting different initial states $(x_0, y_0, z_0, w_0, v_0)$ from those used, i.e., $(1, 1, 1, 1, 1)$, may drive the system to a non-chaotic regime, potentially weakening the security of the generated S-Boxes.

The paper "FPGA Implementation of Modified SNOW 3G Stream Cipher Using Fast and Resource Efficient Substitution Box" [53] presents an approach to the hardware implementation of the SNOW 3G stream cipher, widely used in mobile communications, which employs two 32×32 -bit S-Boxes not derived from a chaotic map. The authors propose a modified hardware implementation of these S-Boxes using logic gates (9 AND, 7 OR, 6 XOR, and 4 NOT gates) instead of conventional implementations based on LUT or *Block Random-Access Memory* (BRAM).

In [53], the proposed SNOW 3G stream cipher architecture is based on sixteen LFSRs, each holding 32 bits; one *Finite State Machine* (FSM) consisting of three registers, each holding 32 bits; and two 32×32 -bit S-Boxes, all utilized in the *Key Initialization* and *Key Generation* processes. The architecture was implemented on a Zynq ZC702 FPGA platform, and its performance was analyzed in terms of area, power consumption, and efficiency. Comparisons were made with four designs found in the literature (employing different FPGA platforms), as well as with an in-house design using a traditional LUT implementation on the same Zynq ZC702 FPGA

platform. Results indicate that the proposed architecture consumes fewer slices, reduces critical path delay, and increases throughput. Furthermore, the proposed design demonstrates higher efficiency in terms of throughput per slice.

The paper "Image Encryption Based on Improved Lorenz System" [46] introduces an image encryption scheme based on an enhanced Lorenz chaotic system. The proposed map preserves the original Lorenz system's three-dimensional structure and the nonlinear terms $x \cdot z$ and $x \cdot y$ from Lorenz's seminal work [6], as expressed in equation (2.3), while augmenting them with a delay coupling ($\tau = 1$) and a modulo operation ("mod", which returns the remainder of a division between two operands). Consequently, the improved chaotic map demonstrates enhanced ergodicity (its attractor more uniformly occupies the entire state space) and a more homogeneous temporal evolution of its internal states, under the same initial conditions $(x_0, y_0, z_0) = (0.01, 0.02, 0.02)$ and parameters $(a, b, c) = (20, 50, 8)$.

The modified Lorenz-type chaotic map in [46] is further assessed through approximate entropy, information entropy, autocorrelation, frequency distribution, and the NIST SP800-22 suite of fifteen statistical tests. All evaluation results suggest high-quality randomness and complexity of the enhanced Lorenz chaotic map.

The proposed encryption scheme in [46] utilizes this improved chaotic system within a ten-step algorithm that operates without relying on S-Boxes as the primary source of nonlinearity and confusion. Instead, the algorithm employs a sequence of chaos-based confusion and diffusion operations, which are reversed during decryption. However, a notable limitation of this approach is its dependency on the plain image to derive the encryption key, which potentially compromises key secrecy.

Experimental results in [46] were obtained by applying the proposed encryption and decryption algorithm to four distinct plaintext images, analyzing the histograms of both encrypted and decrypted outputs, the latter exhibiting nearly flat distributions as expected. The security analysis included key sensitivity, examining the impact of a one-bit error; and keyspace size ($2^{232} \gg 2^{100}$), which prevents practical brute-force attacks. Statistical evaluation involved computing correlation coefficients between horizontal, vertical, and diagonal pairs of 3,000 randomly selected adjacent pixels, compared with five other algorithms from the literature; information entropy comparisons; differential attack resistance measured by NPCR

and UACI; and robustness testing under data loss, data modification, and salt-and-pepper noise attacks. The proposed algorithm performed well across all tests and analyses, demonstrating strong security properties.

The paper "A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box, and Image Compressing" [45] presents an approach to enhancing the security of image data transmission by combining chaotic systems, S-Boxes, and image compression techniques. This work can be categorized into four algorithmic contributions: novel architecture, improved chaotic dynamics, multi-plaintext image processing, and enhanced encryption speed. Classical one-dimensional chaotic systems (such as Logistic, Sine, and Tent maps) often exhibit weaknesses that are mitigated in this study through the adoption of two compound chaotic systems: the two-dimensional Logistic-Sine-Coupling chaotic map (*2-D Logistic-Sine-Coupling chaotic Map* (2D-LSCM)) and the one-dimensional Sine-Tent piecewise system (*1-D Sine-Tent piecewise chaotic System* (1D-STs)). The proposed encryption algorithm consists of three core phases (combination, scrambling, and diffusion) distributed across eleven steps. Three plaintext images P_i are compressed and combined with a fourth random image R , generated via 2D-LSCM, where R is discarded after decryption. The chaotic sequence is iterated for $T_0 = 100$ steps to eliminate transient effects, with the chaotic parameter θ_0 randomly selected from the interval $[0, 1]$ for each encryption process, ensuring that identical plaintexts produce different ciphertexts at different times and improving resistance to CPA. The resulting bidimensional combined image C undergoes zigzag-pattern scrambling before being processed through a nonlinear S-Box constructed using the 1D-STs chaotic map along with the MATLAB functions `MOD` and `SORT`.

The security performance of the method proposed in [45] is compared against five algorithms from the literature using various criteria: resistance to CPA, keyspace size ($2^{561} \gg 2^{100}$), key sensitivity, MSE, histogram uniformity, the Kolmogorov-Smirnov goodness-of-fit test (MATLAB), correlation coefficients (horizontal, vertical, and diagonal), local information entropy, compression effectiveness, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), robustness against noise and data loss, encryption quality via the Gray-Level Co-occurrence Matrix (GLCM), and computational complexity. However, three notable limitations

are identified: the keyspace estimation does not consider initial conditions that may drive the 2D-LSCM and 1D-STC systems into non-chaotic regimes; the use of parameter T_0 lacks a thorough analysis of transient dynamics in the 2D-LSCM; and the proposed S-Box is not independently evaluated in terms of statistical properties or bijectivity.

The paper "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step" [48] presents four main contributions: (i) a novel technique for chaos-based image cryptography, referred to as Dynamic Encryption Step; (ii) the use of low-dimensional (1-D) chaotic maps in S-Box construction; (iii) pixel diffusion through modification of the statistical characteristics of the encrypted image; and (iv) an extended S-Box size of 10×26 to support more complex image encryption applications. The single S-Box is constructed using iterations of the one-dimensional Logistic map (2.2), with initial condition $x_0 = 0.32568$ and control parameter $\mu = 3.95$, generating a chaotic sequence of 256 distinct values used to populate the 10×26 S-Box, with the last four positions left unused. For a given plaintext image A of size $m \times n = 256$, the algorithm uses each pixel value to index the S-Box, which initially results in high correlation that is mitigated by the proposed Dynamic Encryption Step, parameterized by the total encryption time t . This parameter t defines the number of recursive addressing cycles into the S-Box based on the pixel values of image A . A final pixel diffusion stage is applied by iterating the Logistic map to generate a new chaotic sequence Q and performing an XOR operation with the cipher image C , yielding $C' = C \oplus Q$.

Experimental analysis was conducted in [48] using MATLAB R2018a and four standard test images from the *University of Southern California (USC) Signal and Image Processing Institute (SIPI)* database (Lena, Baboon, Peppers, and Boat), evaluating histogram distribution, χ^2 , correlation coefficients (horizontal, vertical, and diagonal), NPCR, UACI, entropy, robustness to Gaussian and salt-and-pepper noise, robustness to data loss, keyspace size, key sensitivity, and encryption time (in seconds). The results were compared with five related methods from the literature and demonstrate favorable performance. A notable limitation of this work concerns data loss: the portion of the cipher image lost directly corresponds to the portion lost in the decrypted image. In contrast, other approaches (e.g., [45]) diffuse the

effect of data loss across the entire image, improving recoverability.

The paper "A Novel Design of Cryptographic SP-Network Based on Gold Sequences and Chaotic Logistic Tent System" [42] integrates chaotic systems and Gold sequences to overcome their individual limitations and generate high-dimensional chaotic pseudo-random number sequences that are highly sensitive to multidimensional initial conditions, thereby enhancing cryptographic robustness. The proposed SPN (Substitution-Permutation Network) comprises three cryptographic primitives: S-Box, *Permutation-Box* (P-Box), and random key sequences (including a key whitening operation). It operates on 256-byte plaintext blocks, with two rounds (XOR, S-Box, P-Box) followed by a final key addition operation (XOR). An enhanced Logistic-Tent chaotic system (*1-D Logistic Tent chaotic System* (1D-LTS)) generates 256-sized key sequences. Confusion between plaintext and subkeys is achieved using two 16×16 S-Boxes (one per round), constructed via a 15-step algorithm utilizing chaotic Gold sequences, Logistic map, Tent map, and 1D-LTS sequences, applied through a linear fractional transformation of the form $f(z) = (az + b)/(cz + d)$. In parallel, diffusion is realized by two key-dependent P-Boxes (one per round), generated by selecting the first 256 distinct values obtained from an XOR operation between the Gold sequences and the 1D-LTS sequences, as derived in steps 5 and 8, respectively, of the S-Box construction algorithm.

The proposed method in [42] is evaluated through statistical analyses including NL, BIC, SAC, NPCR, UACI, LAP, DAP, histogram distribution, and correlation coefficients computed over 1,000 randomly selected adjacent pixels in horizontal, vertical, and diagonal directions. The two designed S-Boxes exhibit NL equal to 112, which is equal to or greater than that of 30 similar S-Boxes reported in the literature. NPCR and UACI metrics were also compared with eight equivalent cipher techniques, showing favorable results. However, the authors do not specify the initial conditions and chaotic parameters used in the algorithms, nor evaluate whether the chosen parameters ensure that the maps remain in a chaotic regime. Additionally, the decryption algorithm is not described in detail.

The paper "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps" [44] is a clear and well-structured work. It presents a robust and generic cryptographic framework to enhance medical image

security using chaotic systems and dynamically generated S-Boxes. The communication channel is assumed to be lossless in this study. The proposed encryption framework accepts two inputs: the encryption key ($K = K_S \cup K_C$) and a randomly generated number ($N = N_S \cup N_C$), both processed by two generic components: a key-dependent S-Box construction algorithm, denoted $\mathbb{S}_{K_S}$, where $\mathbb{S}_{K_S}(N_S)$ generates two 16×16 bijective S-Boxes; and a chaotic pseudo-random source, denoted $\mathbb{C}(IV)$, iterated N_T times to bypass the transient effect, with the initial vector computed as $IV = AES_{K_S}(N_C)$, yielding a pseudo-random byte stream M used in encryption via XOR operations. The framework employs two XOR operations: first, a plain image pixel is XORed with the previous cipher image pixel; the result is then substituted through the S-Box S and subsequently XORed with the corresponding chaotic mask sequence value M . The random values N_S and N_C are regenerated for every plain image I and must be transmitted alongside each cipher image I_C . During decryption, N_S and N_C are extracted from I_C and used with the shared secret keys K_S and K_C to reconstruct the corresponding chaotic sequence M and inverse S-Boxes. To demonstrate the application of the proposed generic framework, the authors present a sample implementation of the key-dependent S-Box construction component $\mathbb{S}$ based on the Mersenne Twister pseudo-random number generator (PRNG) MT19937. The generic chaotic source component $\mathbb{C}$ is implemented using eight different 2-D chaotic maps found in the literature (Arnold Cat, Baker, Henon, Standard, SLM, SCSLM, SCH, and LSMCL), where the final state (x_{N_T}, y_{N_T}) is converted into 8-bit values for masking.

In [44], performance is evaluated using three medical images and eight chaotic systems, applying analyses including histogram analysis, χ^2 , cross-correlation, spatial correlation (horizontal, vertical, and diagonal), global entropy, local Shannon entropy, NIST randomness tests, texture features (GLCM contrast, correlation, energy, and homogeneity), differential attack metrics (UACI and NPCR), key sensitivity (measured via correlation, UACI, and NPCR), keyspace analysis, resistance to chosen-plaintext (CPA) and chosen-ciphertext (CCA) attacks (evaluated via histogram analysis, χ^2 test, spatial correlation, and entropy of all-white and all-black images), Java implementation runtime, and comparison with over eight related schemes from the literature. The proposed framework achieves high throughput

and enhanced resistance to CPA, CCA, and reset attacks. Limitations include the definition of N_T (the number of iterations used to bypass transient dynamics of the chaotic system) and the keyspace estimation, both of which may vary depending on the specific chaotic map used, as this work evaluates eight different maps.

Mohamed et al. [173] present a novel image encryption algorithm designed to enhance the security of multimedia data transmitted over insecure channels. The proposed method relies on the construction of DNA-coded fuzzy substitution boxes (DNAFZ S-Boxes) and their integration with hyper-chaotic maps. Unlike conventional image encryption approaches, which struggle with large data volumes and often require specialized architectures, the proposed scheme leverages *Choquet Fuzzy Integral* (CFI) and DNA operations to generate DNAFZ S-Boxes with strong cryptographic properties, thereby achieving high security and randomness. The encryption process begins with shuffling the 8-bit binary representation of the plaintext image using an M-sequence, followed by down-sampling into four sub-images. These sub-images are then subjected to pixel substitution based on the constructed DNAFZ S-Boxes. A diffusion phase is subsequently applied, in which each DNAFZ-encoded sub-image is diffused using a distinct DNA-encoded chaotic sequence generated by Chen’s hyperchaotic system. The initial parameters of Chen’s system are carefully selected to ensure strong chaotic behavior. Owing to the inherent sensitivity of hyper-chaotic systems to initial conditions, the generated sequences exhibit high unpredictability, thereby reinforcing the cryptographic strength of the algorithm. Finally, the four diffused sub-images are merged to form the encrypted image. Extensive numerical simulations and cryptographic analyses—including correlation, homogeneity, energy, entropy, and resistance to attacks such as chosen-plaintext and differential attacks—demonstrate the robustness and effectiveness of the proposed approach. The experimental results highlight its superiority over conventional schemes, with encrypted images achieving near-ideal statistical metrics, including very low pixel correlation coefficients and entropy values close to the theoretical maximum of 8.

To conclude this section, Table 3.3 summarizes the systematic bibliographic review presented in Section 3.3.2, covering more than 25 works addressing chaos-based cryptography, encryption schemes, and S-Box design. The table consolidates

bibliometric information, cryptographic design characteristics, and evaluation metrics, enabling a structured comparison across different approaches. In particular, three key methodological parameters are analyzed: K_s , which indicates whether the key space estimation is grounded on the volume of valid initial conditions of the underlying chaotic system; T_T , which identifies whether transient dynamics are explicitly considered in the system initialization phase; and OtF, which distinguishes between schemes that precompute chaotic sequences and those that generate them on-the-fly during encryption. The consolidated results reveal that none of the surveyed works simultaneously address these three aspects in a systematic manner, highlighting a persistent methodological gap in the literature that motivates the contributions of this thesis.

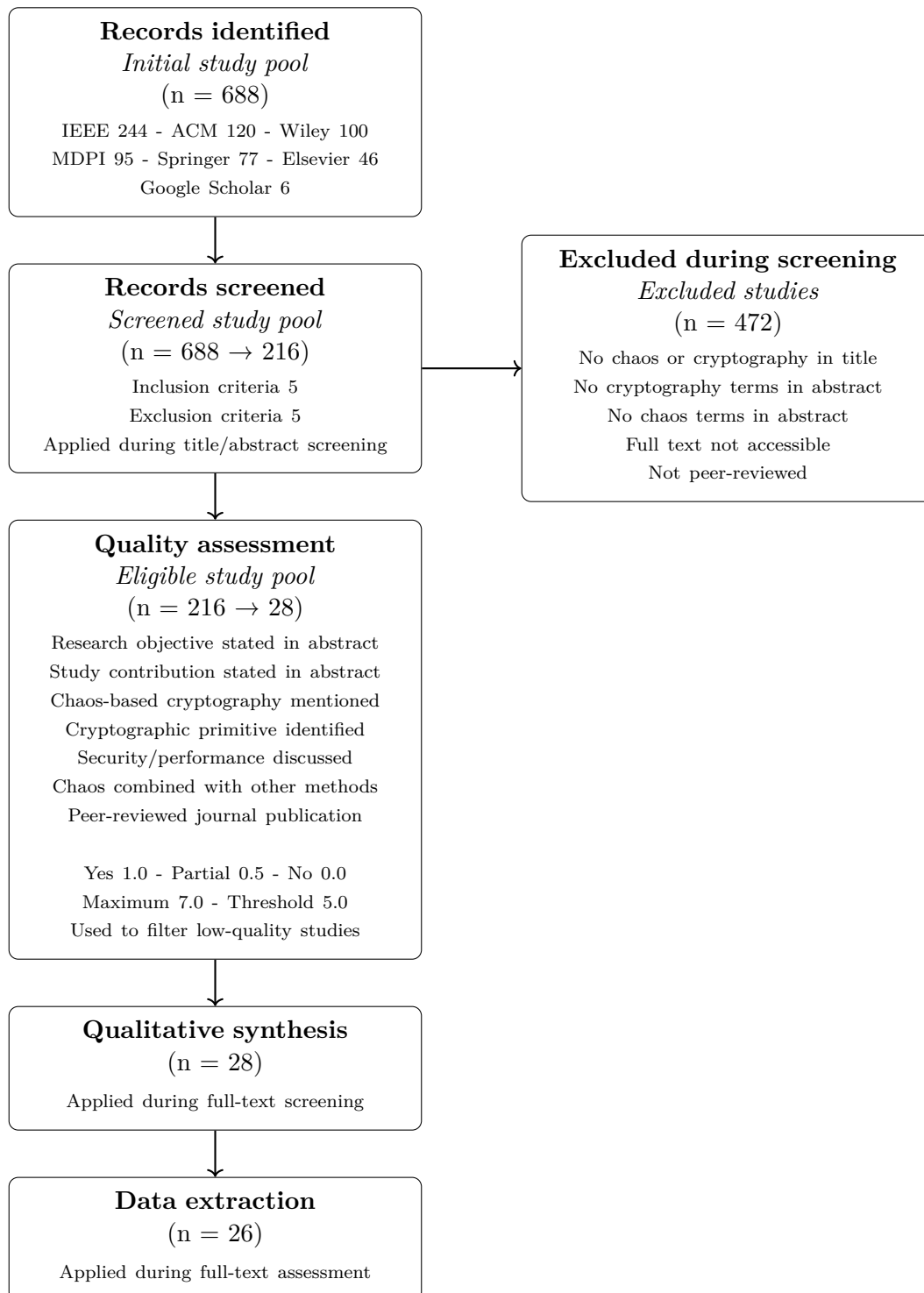


Figure 3.2: PRISMA diagram of study selection in the SLR

Table 3.3: Selected primary studies for the SLR

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
1998 Kocarev [22] Macedonia Conference IEEE	4pg 8rf 15 15 23 25 years 7 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Partitioning the state space of the Hyperbolic chaotic map, and applied to a Feistel symmetric block cipher	No application domains are specified, it deals only with bits	No platforms HW/SW are specified, it deals only with the algorithm	S-Boxes are not part of this study	Counting number of bits changing for different plaintext of cipher keys
2001 Jakimoski [24] USA Journal IEEE	7pg 40rf 15 15 23 25 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	A 8-bit S-Box, based on the Logistic and Exponential chaotic maps, applied to a Feistel block cipher	No application domains are specified	Easy imple- mentation (HW/SW) because it uses byte operations	Linear and differential probability bias; and bijectivity forced during construction	Preliminary results (not reported) indicate it has good cryptographic properties
2005 Tang [29] China Journal Elsevier	9pg 27rf 19 18 75 21 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = Yes	120 8-bit S-Boxes based in skew tent chaotic maps, obtained by changing IC and iteration time	No application domains are specified	No platforms HW/SW are specified	Bijectivity, Nonlinearity, SAC, BIC, Equiprobable input/outup XOR distribution	Criteria for good S-Boxes fulfilled implying immunity to resist differential cryptanalysis

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2012 Peng [37] China Journal IGI Global	20pg 31rf 2 2 6 14 years 7 score 2 grade	4D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	500 key-dependent dynamic 8-bit chaotic S-Boxes generated using Hyperchaotic Lorenz System	Cognitive informatics, exemplified by digital image encryption	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC, DP_f	Histogram and correlation of 2000 pairs of horizontal adjacent pixels
2014 Guesmi [38] Tunisia Conference IEEE	7pg 33rf 26 26 46 12 years 7 score 3 grade	1D + 3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Logistic map for initial 8-bit S-Box and Lorenz chaotic system for genetic algorithm control parameters	No application domain are specified	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC	The cipher was neither implemented nor evaluated
2017 Rashmi [40] India Journal ISROSET	13pg 21rf 0 0 0 9 years 7 score 1 grade	2D + 2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Self adaptive image encryption technique based on Logistic and Arnold maps without S-Boxes	Image encryption by pixel permuta- tion and diffusion	Intel(R) Pentium(R) 2.30 GHz with Matlab 7.0	The S-Box was neither implemented nor evaluated	Histogram, correlation, entropy, MSE, NPCR, PSNR, UACI, speed of encryption

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2019 Khan [42] Pakistan Journal IEEE	12pg 59rf 25 25 27 7 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	SP-Network based on Gold Sequences and chaotic Logistic Tent systems using S-Box and P-Box	Color image encryption	No platforms HW/SW are specified	Nonlinearity, BIC, SAC, NPCR, UACI, Linear and Differential approximation probability	Histogram and adjacent pixel correlation analysis of 3 images (Lena, Baboon, and Pepper)
2019 Yi [174] China Journal IEEE	12pg 23rf 38 38 87 7 years 5 score 5 grade	1D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Block cipher, Feistel network, 16 x 16 S-Box, compound and sinusoidal chaotic maps, Baker map, linear congruence generator	Wireless sensor networks	CC2430 <i>System-on-a- Chip</i> (SoC) platform, 8051 MCU 32 MHz, 128K flash, 8K RAM	Bijectivity by construction, NL, SAC, BIC, LAP, DAP, <i>Maximum</i> <i>Expected Linear</i> <i>Probability</i> (MELP)	keyspace, 0 and 1 balance, entropy, NIST, diffusion and confusion analysis, speed and storage

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2020 Ahmad [43] India Journal IEEE	15pg 85rf 39 37 62 6 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hybrid-constructed S-Boxes (5–8 bit; 4×8–16×16) using Ahmad’s improved chaotic map and algebraic group operations (MOD, SIN, and POWER)	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC-NL, LAP, DAP	Histogram and MLC
2020 Ibrahim [44] Saudi Arabia Journal IEEE	17pg 56rf 90 62 90 6 years 7 score 5 grade	2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	A hybrid of Block Cipher (PRNG MT 19937), Stream Cipher (chaotic maps: Baker, Henon or other) and 8-bit S-Box	Medical image encryption	JavaSE 1.8 virtual machine, Intel Core i7-4790, 3.6GHz, 32GB RAM	Bijectivity by construction, nonlinearity, BIC, SAC, Differential Uniformity, LAP	Histogram, correlation, entropy, NIST, texture, UACI, NPCR, CPA, CCA, key sensitivity, keyspace, speed

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2020 Lidong [45] China Journal IEEE	18pg 58rf 37 12 37 6 years 7 score 5 grade	2D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hibrid encryption combining compression, 2D-LSCM chaos and 16 x 16 1D-STS-based S-Box	Image encryption	MATLAB 2018b, Intel(R) Core(TM) i7-8550U, 8G RAM, WIN 10 Enterprise	No S-Box evaluation	CPA, keyspace, key sensibility, histogram, correlation, entropy, noise and data loss, GLCM, time complexity
2020 Zou [46] China Journal IEEE	13pg 44rf 46 16 46 6 years 7 score 4 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Encryption with a improved (nonlinear kinetic complexity and ergodicity) of Lorenz system	Color Image encryption	No platforms HW/SW are specified	No S-Box was implemented	Key security, keyspace, correlation, entropy, DAP, noise attack, data loss

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2020 Ibrahim [175] Saudi Arabia Journal IEEE	14pg 83rf 44 43 77 6 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	PRNG, ECC, Henon chaotic map, 16 x 16 S-Box	Image encryption	CPU Core-i7- 8565U 1.8 GHz, 12GB RAM, MATLAB	Bijectivity by construction, NL, LAP, DAP, SAC, BIC-SAC	Histogram, χ^2 , correlation, entropy, key and plaintext sensitivity, NPCR, UACI, BFA, CPA, CCA, speed
2021 Maadeed [47] Qatar Journal Springer	22pg 46rf 14 14 57 5 years 7 score 4 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Stream cipher, 16 novel static 8-bit polynomial S-Boxes, and a new chaotic encryption algorithm	Image encryption	MATLAB, Windows 10, i5 CPU, 8GB RAM	Bijectivity by construction, nonlinearity, BIC, SAC, LAP, DAP	Correlation, entropy, contrast, homogeneity, energy, keyspace, key sensitivity, NPCR, UACI, noise, data loss, LAP, DAP, speed

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2021 Jun [48] China Journal IEEE	17pg 53rf 39 39 39 5 years 7 score 4 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Block Cipher, 10×25 Logistic-based S-Box, with a dynamic encryption step	Image encryption	MATLAB 2018a, AMD Ryzen 5, 2.10 GHz, 8GB RAM, WIN 10	Bijectivity by construction	Histogram, χ^2 , correlation, UACI, NPCR, LAP, DAP, entropy, noise (Gaussian, Salt, Pepper), data loss
2021 Mohamed [173] Egypt Journal IEEE	23pg 68rf 42 42 54 5 years 6 score 5 grade	4D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	PRNG, 16 x 16 S-Box, Chen's hyperchaotic system, Choquet fuzzy integral, DNA sequences	Image encryption	CPU 3.0 GHz, 8GB RAM, Windows 10, MATLAB R2017b	MLC, entropy, correlation, energy, Homogeneity	Key sensitivity, histogram, NIST, χ^2 , information entropy, correlation, NPCR, UACI, PSNR, contrast, speed, robustness

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2021 Ramzan [176] Pakistan Journal IEEE	24pg 51rf 16 16 40 5 years 4 score 4 grade	NA $K_S = \text{No}$ $T_T = \text{NA}$ $OfF = \text{No}$ Degrad = NA	SPN, ECC based S-Box, no chaos map is used	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, NL, LAP, SAC, BIC, DAP	Key sace and sensitivity, NPCR, UACI, entropy, χ^2 , correlation, histogram, MSE, PSNR
2021 Hernandez [177] Mexico Journal MDPI	25pg 40rf 5 5 13 5 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Symmetric encryption, block cipher, ECC, Logistic map, PRNG	Color image encryption	Intel Core i3 7350k, 4.0 GHz, dual-core, 8 GB RAM, HD SATA 7200 RPM, Windows 10 Pro	NL, algebraic degree and immunity, balance, correlation, DAP, SNR, power analysis, transparency order, correlation, etc.	Entropy, correlation, χ^2 , NPCR, UACI, avalanche effect, CPA, KPA, keyspace and sensitivity, data loss, noise attack, speed

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2022 Manzoor [5] Pakistan Journal IEEE	11pg 60rf 21 21 38 4 years 7 score 4 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	New MAZa chaotic map for design of dynamic 16 x 16 S-Boxes using a heuristic method	No application domain are specified	Visual C#, Windows 8, Intel core i7 CPU, 2.2 GHz, 4GB RAM	Bijectivity by construction, nonlinearity, fixed points, SAC, BIC, LAP, DAP	Keyspace
2022 Nazir [50] Pakistan Journal IEEE	16pg 94rf 16 16 27 4 years 7 score 5 grade	4D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hybrid DNA Encoding (Logistic map), Hash function, block cipher (Hyperchaos), and S-Boxes ($16 \times$ 16)	Color image ($M \times N$) encryption	Matlab R2015a, Intel i7-1165G7, 4.7 GHz, 8 GB RAM, Windows 8	Nonlinearity and SAC	PSNR, MSE, NIST, keyspace, key sensitivity, DAP, NPCR, UACI, correlation, histogram, GLCM, entropy, CPA, MAE, noise, data loss

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2022 Haque [178] India Journal IEEE	15pg 63rf 4 4 26 4 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Symetric cipher, 16 x 16 S-Box, <i>Piecewise Linear</i> <i>Chaotic Map</i> (PWLCM) chaotic map, 2D cellular automata, algebraic structures	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, NL, DAP, LAP, SAC, BIC-NL, correlation	Histogram, MLC
2022 Tian [179] China Journal MDPI	25pg 78rf 12 12 32 4 years 5 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	16 x 16 S-Box, modified discrete chaotic map, Arnold transformation, DRPE	Image encryption	CPU i5-9400, 2.9 GHz, 16 GB RAM, Windows 7, MATLAB R2012b	Bijectivity by construction, NL, SAC, BIC, BIC-NL, BIC-SAC, LAP, DAP	keyspace and sensibility, histogram, χ^2 , MSE, PSNR, correlation, NPCR, UACI, data loss, noise attack, entropy, speed

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2023 Goswami [53] India Journal IEEE	4pg 13rf 2 2 5 3 years 7 score 4 grade	NA $K_S = \text{NA}$ $T_T = \text{NA}$ $OfF = \text{NA}$ Degrad = NA	Stream Cipher, 32x32 bits S-Box in boolean function (no LUT, no chaos), Key Generation, LFSR, FSM	4G LTE security ap- plications, focusing on area, power, and efficiency	Implemented on FPGA Zynq ZC702	No S-Box evaluations are performed (only FPGA resources utilization)	No cipher evaluations are performed (no encryption was realized)
2023 Zhang [52] China Journal MDPI	23pg 49rf 1 1 7 3 years 7 score 4 grade	2D $K_S = \text{NA}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = Yes	PRNG, hyperchos-based 16 x 16 dynamic S-Box, hybrid with quantum randow walks	Image encryption and video authenticata- tion (future work)	No platforms HW/SW are specified	Bijectivity by construction (swapping), nonlinearity, SAC, BIC, DAP, LAP, security, etc.	No cipher evaluations are performed (no encryption was realized)

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2024 Alabdullah [56] Saudi Arabia Journal IEEE	12pg 45rf 0 0 3 2 years 7 score 4 grade	5D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Key Stream, 16 x 16	Information security,	No platforms HW/SW are specified	Bijectivity by construction (Delannoy Numbers), nonlinearity, SAC, BIC, LAP, DAP	No cipher evaluations are performed (no encryption was realized)
			S-Box based on Delannoy numbers and Bashir's multiwing hyperchaotic system	data protection, and secure communica- tion (future work)			
2024 Ibrahim [57] Saudi Arabia Journal IEEE	12pg 37rf 4 0 4 2 years 7 score 5 grade	2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	PRNG-based 12-bit		Java VM 1.8,	Bijectivity by construction (no further evaluation is provided)	Histogram, entropy, correlation, χ^2 , NPCR, UACI, key sensitivity, keyspace, CPA, speed
			key dependent S-Box, 2D Baker chaotic-based stream cipher	Medical image encryption	Intel i7-8565U, 1.8 GHz, 12GB RAM		

Continued on the next page

Table 3.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2025 Dutra [180] Brazil Journal MDPI	28pg 63rf 1 1 1 1 year 7 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{Yes}$ $OfF = \text{Yes}$ Degrad = Yes	A 19-bit S-Box, based on the Sprott B chaotic system (analyzed for encryption application), and applied to a Feistel block cipher	Image and text encryption, applied to Feistel and Hash structures	Xilinx Spartan-3 FPGA, tested using System Generator for MATLAB	Area, power, and timing on FPGA; linear and differential bias computation; and bijectivity	Frequency, throughput, and FPGA resource usage; histogram analysis for image and text data

NOTES — Bibliographic Identification: Year of publication, first author’s surname and reference, country, type of venue (Journal or Conference), publisher; **Bibliometric Information:** Number of pages and references, total citations, mentioning, citing publications (<https://scite.ai/>), age of publication in years, reviewer score, and final grade; **Chaotic details:** Dimensions of chaotic systems used, Keyspace computed from initial conditions (Yes/No), Transient Time calculated (Yes/No), On the Fly chaos computation during encryption (Yes/No), chaos degradation considered (Yes/No); **Primitives Description:** Cryptographic primitives (S-Box, PRNG, block cipher, stream cipher, hash, ECC), the description of the S-Box (size; chaos-based; algebraic; heuristic; none), the chaotic system, and hybrid technologies (DNA, AI, ML, Blockchain, Genetic) used; **Application Domain:** Area where the cryptographic scheme is applied (Military; Satellite; Medical, Image encryption; General-purpose; Other); **Platforms (HW/SW):** Platforms used for implementation and testing; **S-Box Evaluation:** Cryptographic metrics (nonlinearity, bijectivity, SAC, BIC, etc.) and security metrics (linear and differential attacks, etc.); **Cipher Evaluation:** Statistical (histogram, boxplot, scatter, heatmap), tests (chi-square, correlation, entropy, NIST/Diehard), and performance metrics (throughput, latency, memory usage). NA: Not Applicable.

3.3.3 Synthesis and Analysis

The analysis herein consolidates and critically interprets the evidence extracted from the selected studies, as reported in Section 3.3.2, providing a structured and comparative synthesis of the SOTA outlined in Sections 3.3.2.2 and 3.3.2.3. The analysis is organized into six complementary components. First, (i) a descriptive analysis outlines the main bibliometric trends and general characteristics of the reviewed literature. Next (ii), a technical analysis provides a structured comparative evaluation of chaos-based cryptographic designs, including chaotic systems, S-Box construction methodologies, and cipher architectures. This is followed (iii) by an assessment of the evaluation practices and their methodological limitations. Based on these findings (iv), key research gaps are identified, revealing unresolved challenges and underexplored directions in the field. Subsequently (v), a connection between the identified research gaps and the contributions of this SLR is established within the context of the existing literature. Finally (vi), threats to validity and limitations of the present SLR are discussed to contextualize the scope of the conclusions.

3.3.3.1 Descriptive Analysis of the Literature

A total of 688 studies (initial study pool) were identified based on the intersection of the themes of encryption, chaos, and S-Box, as seen in Fig. 3.2. Considering this initial study pool, the majority of publications were obtained from IEEE (244), followed by ACM (120), Wiley (100), MDPI (95), Springer (77), Elsevier (46), and Google Scholar (6), as shown in Fig. 3.3, indicating a strong concentration in engineering- and computer science-oriented digital libraries. In terms of application domains, multimedia and image encryption clearly dominate the literature, accounting for 305 studies and significantly surpassing other categories such as communications and IoT with 41 studies, general cryptography with 177, cryptanalysis with 30, and other (marketing, Geography, Human topics, Gaming, etc.) with 135, as illustrated in Fig. 3.4. The temporal distribution reveals a growth trend in recent years, with a peak observed in 2022 (79 publications), followed by consistently high publication counts in 2023 (67) and 2024 (73), confirming the increasing research interest in chaos-based cryptographic approaches, particularly after 2014, as illustrated in Fig. 3.5. Earlier years exhibited substantially lower publication counts. It

should be noted that the number of publications reported for 2025 (55) corresponds to studies retrieved up to September 17, 2025.

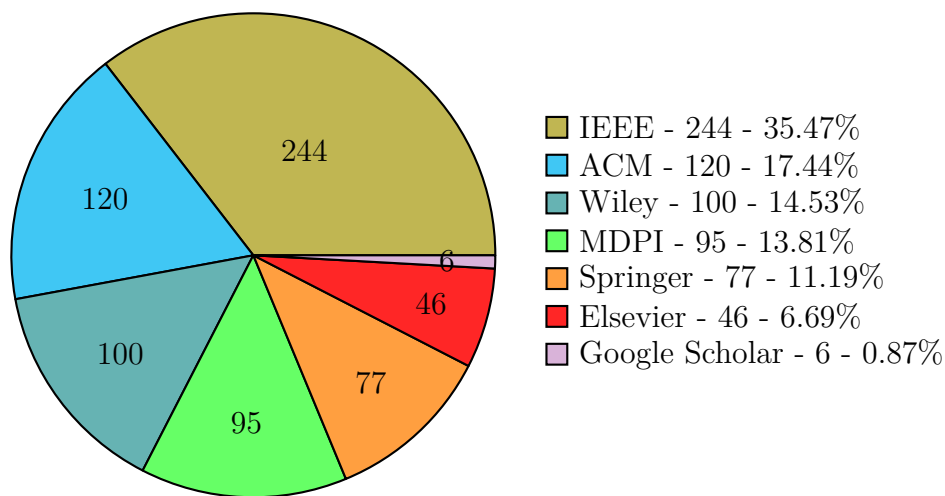


Figure 3.3: Distribution of publication sources in the initial study pool

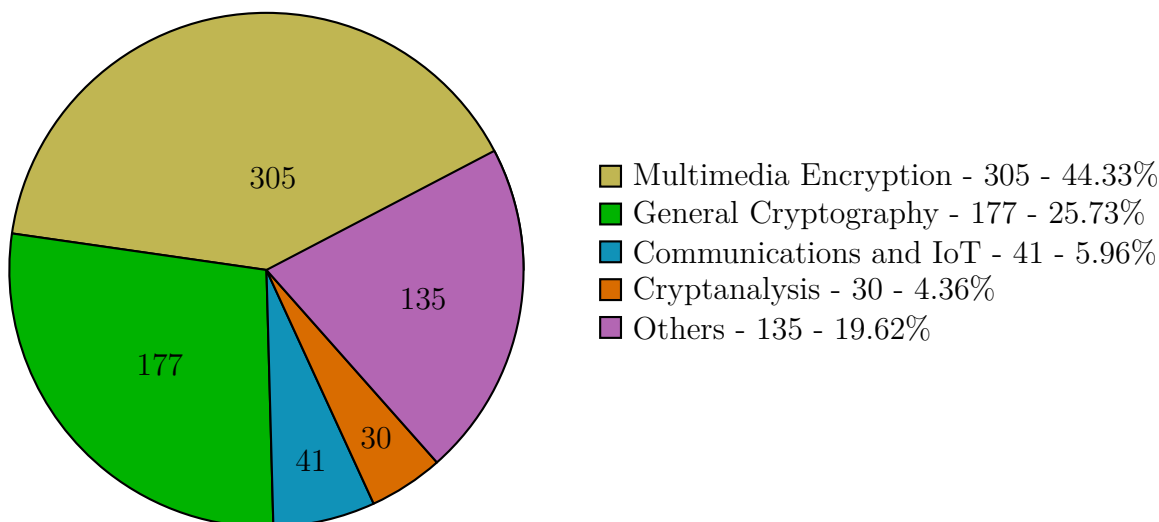


Figure 3.4: Distribution of application domains in the initial study pool

3.3.3.1.1 Excluded Studies

During the initial screening phase, 472 studies from the initial study pool were excluded. The screening process was conducted sequentially across titles, keywords, and abstracts. Abstracts were analyzed only after studies had passed the first two filtering stages (titles and keywords), as they contain more detailed information for evaluation.

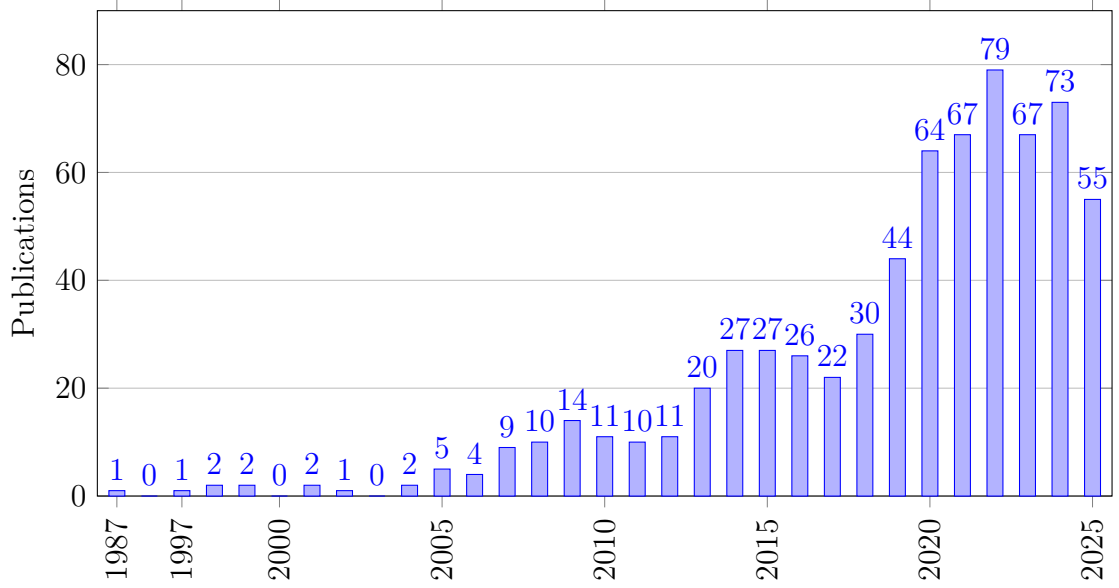


Figure 3.5: Temporal distribution of publications in the initial study pool

The exclusion criteria were applied as follows: studies whose titles indicated no relevance to chaos-based cryptography, chaotic systems/maps, or S-Box design (432 studies); studies with keywords that did not reference chaos or cryptographic concepts (5 studies); and studies whose abstracts did not mention any cryptographic application of chaos or S-Box (35 studies).

From the 472 excluded studies analyzed at the title-based screening stage, a semantic classification revealed a heterogeneous distribution of research topics. The largest proportion of the dataset (28.9%) is dominated by generic “mapping”-related works, including FPGA mapping, schema mapping, and other non-cryptographic uses of the term, introducing significant semantic irrelevance into the search results. The following studies fall under exclusions caused by this category of thematic mismatch: “Functional multiple-output decomposition with application to technology mapping for lookup table-based FPGAs”, which addresses FPGA technology mapping rather than cryptographic primitives; “A mapping system for the integration of OWL-DL ontologies”, which focuses on semantic web ontology integration and schema mapping; and “Towards Trusted Services: Result Verification Schemes for MapReduce”, which is related to distributed computing verification in MapReduce frameworks rather than any cryptographic or chaos-based construction.

The second largest share (18.3%) is related to classical cryptography, encompassing AES, DES, block ciphers, cryptanalysis, and side-channel attacks. These

represent studies excluded due to this category of semantic misalignment: “Neural Networks as a Side-Channel Countermeasure: Challenges and Opportunities”, which addresses side-channel resistance rather than novel cryptographic primitives; “A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks”, which focuses on hardware-level AES protection; and “Compact Designs of SubBytes and MixColumn for AES”, which concerns implementation optimization of the AES structure.

A similar proportion (17.8%) corresponds to chaos-based cryptographic approaches, typically focusing on image encryption or chaotic systems without explicit emphasis on S-Boxes design. These studies were excluded as a result of this type of thematic ambiguity: “Color Image Encryption Algorithm Based on High Dimensional Combination Chaotic System and DNA Coding”, which combines chaos and DNA encoding for image encryption; “A Novel Image Encryption Scheme Based on Chaos and DNA Encoding”, which targets multimedia encryption using chaotic dynamics; and “New Image Encryption Scheme Using Chaotic Maps”, which focuses on generic chaotic encryption without specific S-Box contribution.

Another 17.8% falls into miscellaneous or unrelated domains, such as machine learning, vision systems, and graph-based applications. These are examples of studies excluded due to this category of topical misalignment, including: “YOLO-LPSS: A Lightweight and Precise Detection Model for Small Sea Ships”, which is a computer vision detection model; “DFS-DETR: Detailed-Feature-Sensitive Detector for Small Object Detection in Aerial Images Using Transformer”, which focuses on object detection architectures; and “DGMF: A Unified Dynamic Mapping Framework for Graph Neural Networks”, which is related to graph learning rather than cryptographic systems.

A smaller portion (7.4%) directly addresses S-Boxes construction, optimization, or evaluation, while approximately 3.0% combine chaotic systems with S-Boxes-based cryptographic structures. These examples correspond to studies removed due to this form of scope deviation: “Secure Key-Based Substitution-Boxes Design Using Systematic Search for High Nonlinearity”, which focuses on S-Box design optimization; “Construction and Optimization of Dynamic S-Boxes Based on Gaussian Distribution”, which addresses probabilistic S-Box generation; and “Efficient crypto-

graphic substitution box design using travelling salesman problem and chaos”, which combines combinatorial optimization and chaotic dynamics for S-Box construction.

The remaining 6.8% corresponds to other minor or unclassified areas not covered by the previous categories. These cases illustrate studies excluded on the basis of this category of thematic irrelevance: “Market Prediction in Cryptocurrency: A Systematic Literature Mapping”, which focuses on financial trend analysis; “SeMap: automatic semantic mapping for large-scale indoor spaces”, which addresses spatial semantic mapping; and “Applications of storage mapping optimization to register promotion”, which concerns compiler optimization techniques rather than cryptographic methods.

In addition to the 432 excluded studies analyzed at the title-based screening stage, a total of five studies were rejected due to the absence of explicit references to chaos, cryptographic, and S-Box-related concepts in their keywords. These studies are: “Advanced Encryption Standard Based on Key Dependent S-Box Cube”; “Blockchain-Integrated Secure Healthcare Information Sharing via Advanced Blowfish Encryption Standard With Optimal Key Generation”; “Image Encryption by Chaos Mixing”; “Fast Crown Scheduling Heuristics for Energy-Efficient Mapping and Scaling of Moldable Streaming Tasks on Manycore Systems”; and “S-TPE: Usability Enhanced Thumbnail-Preserving Cryptosystem Based on S-Boxes for Securing IoT-Based Medical Images”.

A total of 35 studies were rejected during the abstract screening stage due to the absence of any mention of cryptographic applications of chaos or S-Box-related concepts. The following are examples of excluded papers: “Random Strip Peeling: A novel lightweight image encryption for IoT devices based on colour planes permutation”, which focuses on lightweight IoT-oriented image encryption using permutation and diffusion mechanisms without explicit consideration of S-Box-based cryptographic design frameworks; “A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images”, which combines chaotic maps with number-theoretic key generation for medical *Digital Imaging and Communications in Medicine* (DICOM) image protection but does not address S-Box-driven substitution mechanisms or related cryptographic primitives; and “On the Telemedicine Microcontroller-Based ECG Security Using a Novel 4Wings-4D Chaotic Oscillator (N4W4DCO)”, which

targets secure biomedical signal transmission using chaotic oscillators embedded in hardware systems, rather than image-based cryptographic constructions or S-Box-oriented encryption schemes.

After completing the screening process based on the inclusion and exclusion criteria, the quality assessment phase was conducted, in which studies were analyzed based on their abstracts, with scores ranging from 0.0 to 7.0. Considering a cutoff score of 4.5, some examples of rejected studies due to low quality are: "A Chaos Based Method for Efficient Cryptographic S-box Design", "A Circuit Design of Discretized Chaotic Maps with Two Iterations for Speeding up S-box Generation", "A Fast Image Encryption Method Based on a Novel One-Dimensional Chaotic Map and Dynamic S-box", "A Method to Construct Dynamic S-box Based on Chaotic Map", and "A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-box Design". These studies were excluded because they failed to satisfactorily meet multiple quality assessment criteria, including the clear definition of the research objective or problem, the explicit presentation of the study contribution, and the clear indication of the use of chaotic systems in a cryptographic context. In several cases, the cryptographic primitive or scheme was weakly specified. Furthermore, many studies did not adequately discuss performance or security aspects and showed limited integration of chaos with complementary techniques such as AI, DNA, and hybrid approaches. Collectively, these limitations indicate a weak alignment with the objectives of the present SLR, justifying their exclusion from the final analysis. Additionally, as part of the quality criteria adopted in this SLR, 65 studies not published in peer-reviewed journals were excluded. After all exclusions, a total of 26 studies were selected for the data extraction phase, which is based on full-text examination.

The Parsifal online tool was instrumental in reducing the initial set of 688 studies to 26 through the screening and quality assessment process. This procedure relied primarily on information available on the first page of each study, such as title, abstract, conference, journal, date, and publication venue, thereby accelerating the review process. For instance, studies such as "A mapping system for the integration of OWL-DL ontologies", which focuses on semantic web ontology alignment and schema mapping, and "Towards Trusted Services: Result Verification Schemes

for MapReduce", which addresses distributed computing verification in MapReduce environments, were excluded due to their lack of relevance to cryptographic systems, chaotic models, or S-Box-based constructions. Similarly, "Neural Networks as a Side-Channel Countermeasure: Challenges and Opportunities" and "Compact Designs of SubBytes and MixColumn for AES" were excluded because they focus on side-channel resistance techniques and optimization of existing AES architectures, respectively, rather than proposing new chaos-based cryptographic primitives or S-Box design methodologies aligned with the scope of this SLR. This approach enabled the selection of a representative and high-quality sample for the data extraction phase, which was based on full-text analysis and operationalized through the use of a structured extraction form.

3.3.3.1.2 Included Studies

This section presents a descriptive analysis of the selected studies, covering their temporal distribution, publication venues, geographic distribution, application domains, implementation platforms, and general trends in chaos-based cryptography.

As illustrated in Fig. 3.6, a clear upward trend in research activity can be observed over time. Approximately 48% of the selected studies were published between 2020 and 2024, indicating a significant increase in interest in chaos-based cryptographic designs. Earlier periods exhibit a comparatively lower concentration of publications, with 20% between 2015 and 2019, while the remaining studies are sparsely distributed between 1998 and 2014.

This upward trend is consistent with broader global patterns in scientific production. Over the same period, the world population has experienced steady growth, increasing from approximately 6.1 billion in 2000 to over 8.0 billion in the early 2020s, corresponding to an increase of more than 30%, thereby expanding the global pool of researchers and potential contributors [181]. In parallel, the volume of scientific publications has grown at an even faster rate, with estimates indicating that the number of peer-reviewed articles has more than doubled since the early 2000s [182]. Major publishers and indexing platforms such as IEEE Xplore, MDPI, and Elsevier have significantly expanded their publication output, with MDPI, for instance, experiencing rapid growth in the last decade driven by its open-access model [183],

while IEEE and Elsevier have continuously increased their digital library coverage and journal portfolios. These technological and institutional developments, combined with the widespread adoption of online submission and peer-review systems, have substantially lowered barriers to dissemination and accelerated the publication process. Therefore, the observed increase in chaos-based cryptographic research is not an isolated phenomenon, but rather reflects a combination of domain-specific interest and a global expansion in scientific output enabled by demographic growth and advances in digital publishing infrastructure.

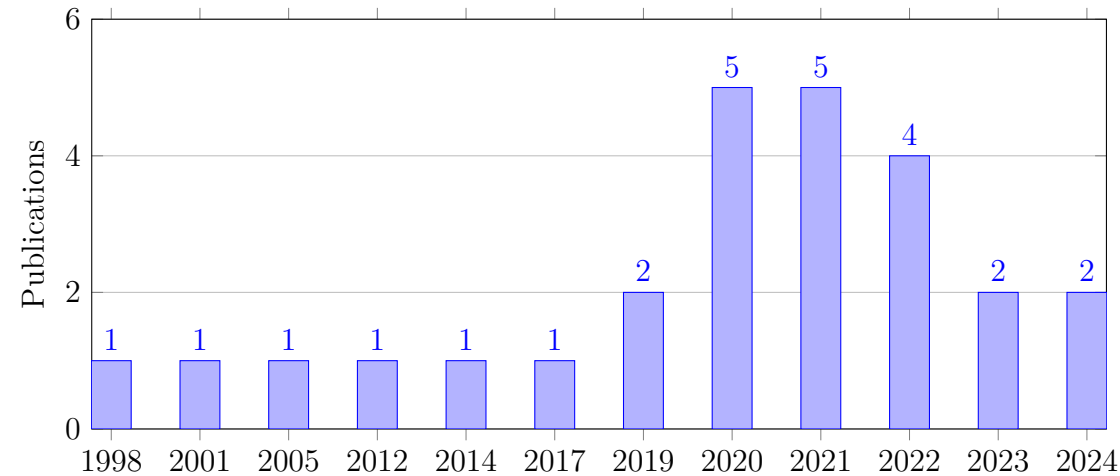


Figure 3.6: Temporal distribution of publications in the included studies

The bibliometric characteristics of the selected studies are summarized in Table 3.3. As illustrated in Fig. 3.7, the geographic distribution is heavily concentrated in Asia, which accounts for approximately 81% of the publications. In contrast, contributions from Europe, Africa, and the Americas remain marginal, representing about 4%, 8%, and 8%, respectively. This pronounced asymmetry indicates that research on chaos-based cryptographic designs is predominantly driven by Asian institutions, while the limited participation from other regions highlights a clear geographic imbalance and suggests opportunities for broader international collaboration.

This pattern is not unique to chaos-based cryptography, but rather reflects a broader trend observed across electrical and electronic engineering research, where Asian countries—particularly China, India, and South Korea—consistently dominate publication output in IEEE- and MDPI-indexed venues. Such dominance has been widely reported in bibliometric studies and indicates a sustained consolidation

of research capacity in the region.

From a demographic perspective, global population distribution is also markedly uneven, with Asia accounting for approximately 59% of the world’s population, followed by Africa (18%), the Americas (13%), and Europe (9%), while Oceania represents less than 1%. This demographic concentration contributes to a larger pool of researchers in Asia and may partially explain the higher volume of scientific output observed in the region.

Nevertheless, although population size is a relevant contributing factor, it does not fully account for research productivity. The strong concentration of publications in Asia observed in this SLR is more accurately understood as the result of multiple interacting factors, including research funding, institutional capacity, technological infrastructure, and national policies that actively promote scientific development.

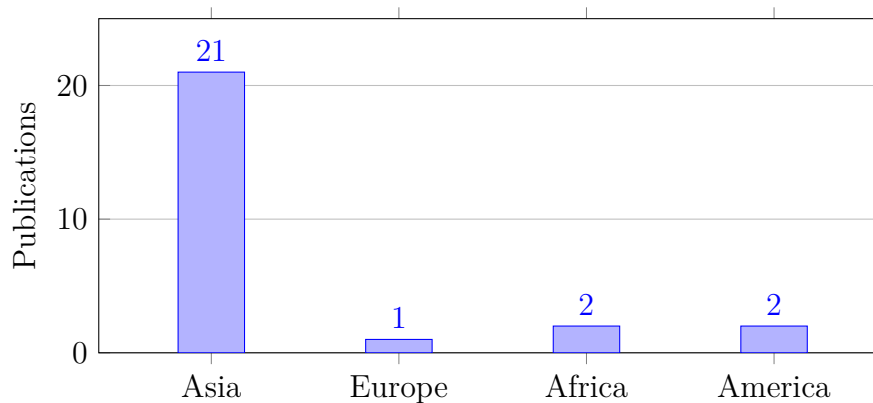


Figure 3.7: Geographical distribution of publications in the included studies

In terms of publication venues, the distribution is markedly skewed toward publications indexed by the IEEE, which account for approximately 73% of the selected studies, as illustrated in Fig. 3.8. The remaining contributions are comparatively limited, with MDPI representing about 12%, while other publishers—such as Elsevier, Springer, IGI Global, and ISROSET—each account for roughly 4% of the total. This pronounced concentration suggests a strong alignment of chaos-based cryptographic research with engineering-oriented venues, in which the IEEE maintains a dominant position due to its established role in electrical engineering, communications, and information security.

It is important to note, however, that during the inclusion and exclusion

process, a substantial number of studies related to chaos were identified in publishers such as Springer and Elsevier (e.g., via ScienceDirect), particularly in journals focused on nonlinear dynamics and entropy. Nevertheless, these works are predominantly oriented toward physics and mathematics rather than engineering-driven cryptographic applications, and were therefore excluded based on the defined selection criteria, namely the focus on S-Boxes in chaos-based encryption.

Regarding the type of publication venue, there is a clear predominance of journal articles, which comprise approximately 92% of the dataset, whereas conference proceedings account for only about 8%. This distribution reflects a preference for more mature and fully developed contributions, as established in the quality assessment protocol of this SLR. Journal publications typically involve more rigorous peer-review processes and more comprehensive experimental validation.

Notably, the few conference papers included in Table 3.3 were retained through the full-text analysis phase of the Parsifal tool due to their relevance to the scope of this SLR. Their inclusion is therefore justified by their conceptual or methodological significance, despite the general preference for journal-based evidence.

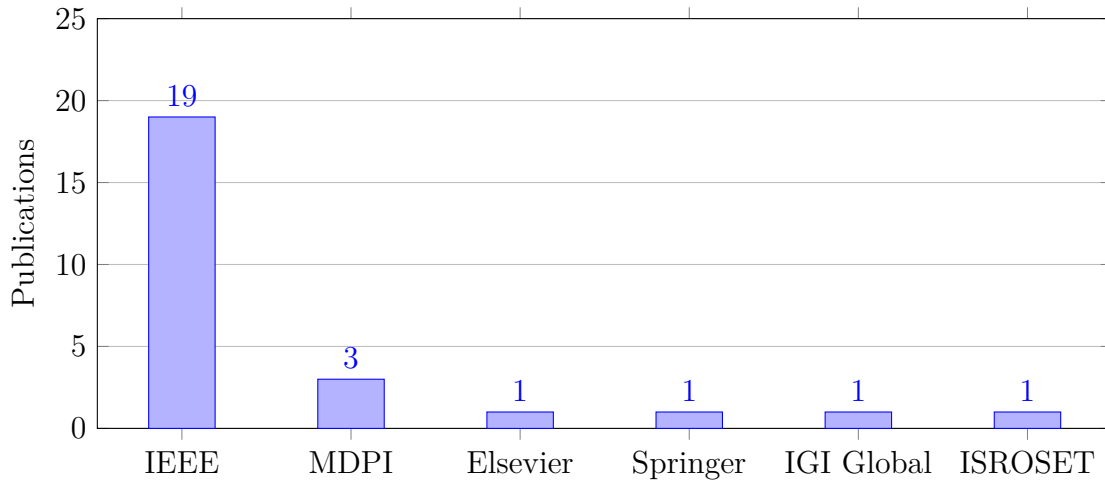


Figure 3.8: Distribution of publications across publishers in the included studies

From a technical perspective, most studies included in Table 3.3 focus on the design and simulation of encryption algorithms, typically implemented in software environments such as MATLAB or general-purpose computing platforms. In contrast, relatively few works explore hardware-oriented implementations, such as those based on FPGA or SoC, indicating a gap between theoretical design and practical deployment.

With respect to application domains, approximately 69% of the studies listed in Table 3.3 focus on chaos-based multimedia encryption applications, predominantly targeting image data (see Fig. 3.9). Image encryption clearly represents the primary application domain identified in the reviewed literature. Most studies employ chaos-based cryptographic techniques for visual data protection, commonly combining substitution–permutation structures with statistical security validation metrics. In contrast, other application domains, including IoT, secure communications, wireless sensor networks, and general-purpose cryptographic primitives, remain comparatively underexplored. This strong concentration on multimedia encryption highlights a significant domain imbalance in current research trends and further emphasizes the relevance of the present SLR, which focuses specifically on chaos-based S-Boxes.

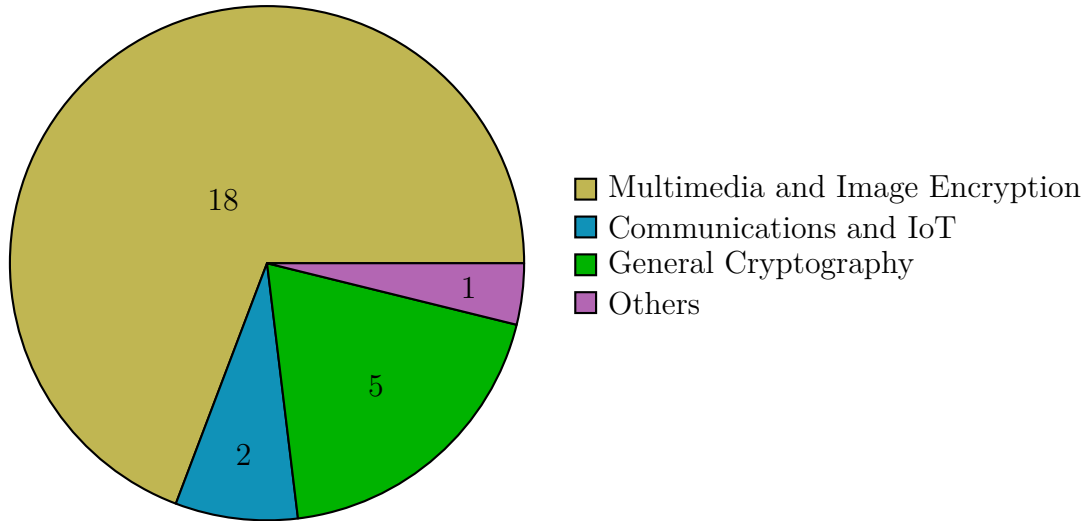


Figure 3.9: Distribution of application domains in the included studies

3.3.3.2 Technical Analysis of Chaos-Based Cryptographic Designs

This subsection provides a structured comparative analysis of the chaos-based cryptographic designs identified in Table 3.3. A unified analytical framework is adopted to systematically evaluate the reviewed studies across four subsections: Chaotic Systems Details, Primitives Description, Implementation Platforms, S-Box and Cipher Evaluation Metrics. More specifically, the analysis investigates: the dimensionality and characteristics of the employed chaotic systems, including hyperchaotic and hybrid constructions, keyspace modeling, transient-state consid-

erations, OtF computation, and chaos degradation effects; the adopted cryptographic primitives and architectural structures, including chaos-based S-Boxes, Feistel and SPN schemes, and hybrid approaches; the implementation platforms employed, with emphasis on the predominance of simulation-based environments versus hardware-oriented realizations; and the cryptographic evaluation methodologies adopted at both the S-Box and cipher levels, including statistical randomness analysis, differential-security metrics, performance-oriented evaluations, and resistance to cryptanalytic attacks.

3.3.3.2.1 Chaotic Systems Characterization

An important step in the design of chaos-based S-Boxes for cryptographic algorithms is the selection of a chaotic system or map suitable for the intended application. As discussed in Section 3.3.2.1, when applying chaos theory to cryptography, several critical and performance-related aspects must be considered, including: the advantages of the selected chaotic system with respect to hardware and/or software implementations [162]; the volume and distribution of valid ICs admitted by the chaotic system or map [2]; and the ergodicity, effective keyspace, and time response of the system [4].

Table 3.3 presents the selected SOTA studies, which constitute the main corpus of the present SLR. Considering the dimensionality of the chaotic maps and systems employed, 34.6% use 1D chaotic models, 11.5% use 2D chaotic models, 15.4% use 3D chaotic models, 7.7% use 4D chaotic models, and 3.8% use a 5D chaotic models [56]. In 7.7% of the studies, chaos is “Not Applicable” [53,176], while 19.2% employ hybrid or composite chaotic systems [38,40,45,50,174]. Hyperchaotic systems are used in 19.2% of the studies, including a 4D Lorenz-type hyperchaotic system [37,50], Chen’s hyperchaotic system [173], a 2D hyperchaotic map [52], and a 5D multi-wing hyperchaotic system [56].

Almost half (46.1%) of the studies employ 1D and 2D low-dimensional chaotic maps and systems, which simplifies implementation and design considerations. Although there is a clear trend toward more advanced techniques as the field evolves, including the use of hyperchaotic systems, characterized by the presence of multiple positive Lyapunov exponents and typically requiring higher-dimensional state spaces, this shift is not yet dominant. There is also a tendency toward hybrid

and composite solutions, which often rely on lower-dimensional chaotic components but enhance overall cryptographic performance by combining them with other techniques, such as DNA encoding, Gold sequences, algebraic group structures, compression techniques, quantum walks, and other related hybrid cryptographic mechanisms.

Table 3.3 also shows whether the Keyspace (K_S) was computed considering the volume of valid ICs for the applied chaotic system or map. In this regard, 0.0% of the studies reported “Yes”, 88.5% reported “No”, and 11.5% were classified as “Not Applicable” [52, 53, 176]. Another investigated aspect concerns the Transient Time (T_T), defined in [4] as the time required for a set of valid ICs to spread throughout the attractor region, which may be interpreted as an indirect measure of chaotic ergodicity. Regarding this aspect, 0.0% of the studies considered T_T , 92.3% did not consider it, and in 7.7% of the studies it was classified as “Not Applicable” [53, 176]. The table 3.3 also investigates whether the encryption designs computed chaotic outputs On the Fly (*OtF*). In this case, 0.0% of the studies reported “Yes”, 96.2% reported “No”, and 3.8% were classified as “Not Applicable” [53]. The SLR further investigates whether chaos degradation was considered during the cryptographic design process. In 84.6% of the studies, chaos degradation was not considered, only 7.7% explicitly addressed degradation issues [29, 52], and in 7.7% of the studies chaos degradation was classified as “Not Applicable” [53, 176].

These four chaos-related parameters (K_S , T_T , *OtF*, and chaos degradation) are important design aspects and must not be neglected in chaos-based cryptographic systems. The use of chaotic maps and systems requires the adoption of valid ICs; otherwise, the expected chaotic behavior will not emerge. This consideration becomes particularly important when the encryption algorithm uses the ICs as part of the cryptographic key, although it also affects other design scenarios.

However, none of the studies summarized in Table 3.3 computed the keyspace (K_S) considering the volume of valid ICs associated with the corresponding chaotic attractor. The transient time (T_T) is completely neglected in several studies [5, 37, 42, 50, 52, 56, 173], while in others it is only superficially addressed. In such cases, the authors [29, 38, 43–45, 47] empirically select an initial number of iterations to be discarded before using the chaotic outputs, without providing a deeper statis-

tical analysis demonstrating that the selected transient interval is sufficient. For this reason, the parameter T_T received a “No” classification for all studies listed in Table 3.3, since none of them fully analyzed or justified the implications of transient behavior on the cryptographic design.

Regarding chaos degradation, this phenomenon is inherently present in digital implementations of chaotic systems, especially when reduced numerical precision is employed. Only 7.7% of the studies explicitly considered degradation effects during the design process [29, 52]. Readers should note that these parameters must be carefully considered during the design stage; otherwise, the resulting cipher may present cryptographic weaknesses.

Regarding the on-the-fly (*OtF*) consideration, this is not a mandatory requirement for a chaos-based cryptographic S-Box design, but it represents a design approach discussed in Chapter 5 and in [180], in which chaotic outputs are dynamically computed during the encryption process instead of relying on precomputed LUTs. It is important to observe that none of the analyzed studies dynamically computed the S-Boxes during the encryption process. Instead, all studies relied on precomputed values generated according to a given algorithm and subsequently evaluated through statistical analyses. Some studies employ hybrid techniques, such as DNA-based methods, to strengthen an initially generated chaotic S-Box, while others modify the internal S-Box values by swapping rows or columns according to the encryption key. Nevertheless, none of the analyzed designs actually computes chaotic outputs on the fly during encryption.

The studies [52, 53, 176] are classified as “Not Applicable” with respect to the K_S analysis considering the volume of valid ICs, since they do not provide a cryptographic design in which the effective keyspace depends on the complete set of valid chaotic initial conditions. In [53], the proposed architecture focuses on the hardware optimization of the conventional SNOW 3G stream cipher structure, including fixed S-Boxes, LFSRs, and FSM components, without defining a cryptographic keyspace associated with a chaotic state space. In [52], although a hyperchaotic system is employed for pseudo-random sequence generation and dynamic S-Boxes construction, the work does not formally define or evaluate a cryptographic keyspace derived from the complete set of valid chaotic states. Similarly, [176] employs elliptic-curve-based

S-Boxes and permutation mechanisms without explicitly associating the cryptographic keyspace with valid chaotic initial conditions.

Regarding the transient time (T_T) analysis, the studies [53, 176] were also classified as “Not Applicable”, since their cryptographic mechanisms do not rely on transient chaotic dynamics as a fundamental operational component. In [53], the proposed method does not employ iterative chaotic maps requiring transient-state suppression prior to pseudo-random sequence generation. Likewise, although [176] incorporates substitution-permutation structures and elliptic-curve-based mappings, the proposed approach does not depend on the temporal evolution of a chaotic attractor whose transient behavior must be statistically analyzed or discarded.

Only [29, 52] explicitly acknowledge or discuss chaos degradation effects during the cryptographic design process, although neither study performs a comprehensive investigation of the phenomenon. In [29], the authors recognize the limitations associated with the discretization of continuous chaotic systems for digital implementation and briefly address the influence of iteration parameters on the generated S-Boxes. Similarly, [52] discusses chaos degradation in the context of the proposed hyperchaotic system and pseudo-random sequence generation. However, both studies provide only superficial considerations, without rigorously evaluating the impact of finite-precision arithmetic, state quantization, attractor degeneration, or non-chaotic operating regions on the long-term cryptographic properties of the generated sequences and S-Boxes. Nevertheless, since these studies explicitly recognize degradation-related issues, they were classified separately from the majority of works that completely neglect the topic.

3.3.3.2.2 Primitives Description

Among the selected studies in Table 3.3, approximately 81% explicitly incorporate S-Boxes as a core cryptographic primitive. Only a limited number of studies investigate chaos-based encryption without employing S-Boxes, such as permutation–diffusion image encryption schemes [40, 46] or chaotic Feistel structures based solely on state-space partitioning [22].

The reviewed literature demonstrates an evolution from early chaos-based block cipher proposals toward increasingly hybridized cryptographic architectures. Initial studies, such as [22, 24, 29], primarily explored direct applications of low-

dimensional chaotic maps to Feistel structures and static 8-bit S-Boxes. More recent studies progressively integrate additional cryptographic primitives and emerging technologies, including DNA encoding, quantum random walks, fuzzy integrals, cellular automata, and algebraic group operations. This trend indicates a growing effort to enhance confusion, diffusion, key sensitivity, and statistical security properties through multilayer hybrid cryptographic frameworks.

Regarding cipher structures, block-cipher-oriented approaches are predominant as expected. Several studies employ Feistel or SPN architectures combined with chaos-based S-Boxes, while others adopt stream-cipher-based designs using chaotic keystream generators or hybrid PRNGs. In particular, dynamic and key-dependent S-Boxes emerge as a recurrent design strategy, appearing in studies such as [5,37,52,57]. Furthermore, most implementations rely on low-dimensional chaotic systems (Logistic, Henon, Baker, Arnold, Lorenz, and PWLCM maps), while only a smaller subset employs 4D and 5D hyperchaotic systems.

Hybrid cryptographic constructions dominate the current SOTA. More than half of the reviewed studies combine chaotic systems with additional primitives beyond conventional substitution structures, including DNA encoding, compression, hash functions, linear congruential generators, polynomial constructions, and ECC. Purely chaos-driven cryptographic designs are comparatively uncommon. Moreover, limited attention is devoted to hardware efficiency, formal cryptographic proofs, standardized keyspace modeling, transient-state analysis, and general-purpose cryptographic applications, highlighting important research gaps that motivate further investigation in this area.

3.3.3.2.3 Implementation Platforms

Table 3.3 reveals a pronounced dominance of software-based simulation environments, particularly MATLAB, corresponding to 30.8% of the implementations [40,45,47,48,50,173,175,179]. Java-based implementations account for 7.7% of the studies [44,57], while 3.8% employ a C# software environment [5]. In contrast, 7.6% report hardware-oriented implementations, including FPGA-based realizations [53] and embedded SoC platforms [174]. The remaining 50% of the studies do not explicitly specify an implementation platform, as they primarily focus on algorithmic design and theoretical validation of chaotic constructions and S-Box-based

primitives, without reporting software execution environments or hardware deployment contexts. This subset typically remains at the cryptographic design level, evaluating properties such as bijectivity, nonlinearity, and statistical randomness without implementation-dependent performance assessment.

The reviewed literature is heavily oriented toward simulation-based validation, with MATLAB serving as the primary platform for evaluating cryptographic performance metrics. This indicates that most contributions remain at the proof-of-concept stage rather than targeting real-world deployment.

Hardware-oriented cryptographic validation is scarce. Only a single FPGA-based study [53] explicitly targets hardware efficiency metrics such as area, power, and resource utilization, while one embedded SoC implementation [174] addresses resource-constrained wireless sensor network environments. This represents a significant gap in the literature, as hardware-level evaluation is essential for assessing real-time feasibility, energy efficiency, and resilience under implementation constraints such as side-channel exposure.

The platform distribution highlights a clear imbalance between simulation-driven research and hardware-validated cryptographic engineering. The majority of studies do not target hardware execution platforms, while only 7.6% report hardware or embedded system implementations. This indicates that, despite the maturity of chaos-based S-Box constructions, their translation into efficient and validated hardware architectures remains a relatively unexplored research direction. Consequently, there is a clear opportunity for future work focusing on FPGA and *Application-Specific Integrated Circuit* (ASIC) implementations.

3.3.3.2.4 S-Box and Cipher Evaluation Metrics

There are two primary approaches for evaluating the quality of a cipher. The first consists in assessing the cryptographic strength of its internal core components, which, in this study, corresponds to the S-Box. This type of evaluation is particularly useful for comparative analyses among different S-Box design approaches and in situations in which the cipher itself is not implemented. The second approach consists in evaluating the performance of the cipher itself, which constitutes the ultimate and most comprehensive assessment criterion. Table 3.3 presents, for each selected study, the metrics adopted for evaluating both the cryptographic properties

of the S-Box and the overall cryptographic strength of the cipher.

There is a concentration of evaluation methodologies around a small subset of cryptographic and statistical metrics. The S-Box evaluation metrics identified in the reviewed studies are primarily focused on the following groups: NL and Bijectivity, which evaluate the capability of the S-Box to generate highly complex nonlinear relationships between input and output values while preserving reversibility; SAC and BIC, which assess the sensitivity of the S-Box to small input perturbations and quantify its avalanche and bit-independence properties; and LAP and DAP, which evaluate the susceptibility of the S-Box to statistical cryptanalytic attacks by measuring the maximum probabilities associated with linear approximations and differential propagation. Overall, these metrics constitute the core set of criteria traditionally used to measure the strength in S-Boxes.

At the cipher level, the evaluation methodology is dominated by image-oriented statistical analyses. The evaluation metrics can be organized as follows: Statistical randomness metrics, including Correlation, Histogram, Entropy, and the χ^2 Test, are suitable in image and multimedia encryption schemes to evaluate the statistical properties of the generated ciphertext and to verify the removal of structural redundancies from plaintext data. Differential analysis metrics, namely NPCR and UACI, are primarily intended to assess the sensitivity of the ciphertext to small variations in the plaintext, and are particularly suitable for image encryption schemes, ensuring strong diffusion and high resistance to differential attacks. Keyspace analysis evaluates the resistance of a cryptographic scheme against brute-force attacks by quantifying the total number of possible keys, thereby reflecting the overall security of the key space. Performance-oriented metrics, particularly relevant for hardware implementations, such as Speed and computational efficiency, assess the practical feasibility of the proposed cryptographic systems in terms of execution time, throughput, latency, and hardware resource utilization. Less frequently, additional metrics such as noise attack resistance, data loss robustness, MSE, and PSNR are used, typically in the context of transmission fidelity and image reconstruction quality, whereas NIST reflects statistical validation of randomness through standardized test suites, while CPA and CCA evaluate formal cryptographic security under adversarial models, assessing resistance against chosen-plaintext and chosen-

ciphertext attacks, respectively.

Tables 3.4 and 3.5 summarize the occurrence frequency of the principal evaluation metrics identified in the reviewed studies.

Table 3.4: S-Box evaluation metrics identified in the reviewed studies

S-Box Metrics	Studies	References
NL	17	[5, 29, 37, 38, 42–44, 47, 50, 52, 56, 174–179]
Bijectivity	17	[5, 24, 29, 37, 38, 43, 44, 47, 48, 52, 56, 57, 174–176, 178, 179]
SAC	16	[5, 29, 37, 38, 42–44, 47, 50, 52, 56, 174–176, 178, 179]
BIC	14	[5, 29, 37, 38, 42–44, 47, 52, 56, 174–176, 179]
LAP	13	[5, 24, 42–44, 47, 52, 56, 174–176, 178, 179]
DAP	14	[5, 24, 37, 42, 43, 47, 52, 56, 174–179]
Others	11	[5, 29, 44, 52, 56, 173, 174, 177]
No S-Box Evaluation	4	[40, 45, 46, 53]

The “Others” category in Table 3.4 encompasses a set of less frequently used S-Box evaluation metrics. These include Differential Uniformity, Fixed Points, Algebraic Immunity and Algebraic Degree, Transparency Order, and Power Analysis Resistance, which are primarily associated with resistance to algebraic, statistical, and side-channel attacks. Additionally, some studies consider statistical descriptors such as Entropy, Correlation, and Energy, as well as structural properties such as equiprobable input/output XOR distribution. Each of these metrics appears in only a small number of studies, providing complementary insights into specific cryptographic properties that are not captured by the main evaluation criteria.

The “Others” category in Table 3.5 groups a set of heterogeneous and less frequently adopted cipher-level evaluation metrics. These include statistical and structural descriptors such as MLC and GLCM-based measures, as well as computational complexity indicators such as time complexity and storage requirements. It also incorporates cryptographic and diffusion-related assessments, including MAE, MSE, diffusion analysis, and avalanche effect evaluation, as well as specific security-oriented measures such as BFA resistance. Although each of these metrics appears in a limited number of studies, they provide complementary perspectives.

Another relevant observation concerns the lack of standardization in evaluation methodologies across studies. Several works report only a subset of cryptogra-

Table 3.5: Cipher evaluation metrics identified in the reviewed studies

Cipher Metrics	Studies	References
Correlation	15	[37, 40, 42, 44–48, 50, 57, 173, 175–177, 179]
Histogram	14	[37, 40, 42–45, 48, 50, 57, 173, 175, 176, 178, 179]
Entropy	14	[40, 44–48, 50, 57, 173–177, 179]
χ^2 Test	7	[48, 57, 173, 175–177, 179]
Keyspace	12	[5, 44–47, 50, 57, 173, 174, 176, 177, 179]
NPCR	11	[40, 44, 47, 48, 50, 57, 173, 175–177, 179]
UACI	11	[40, 44, 47, 48, 50, 57, 173, 175–177, 179]
Speed / Performance	10	[40, 44, 47, 50, 57, 173–175, 177, 179]
NIST Tests	4	[44, 50, 173, 174]
CPA	5	[44, 45, 50, 175, 177]
CCA	2	[44, 175]
Noise Attack Resistance	7	[45–48, 50, 177, 179]
Data Loss Robustness	6	[45, 47, 48, 50, 177, 179]
MSE	3	[40, 50, 179]
PSNR	5	[40, 50, 173, 176, 179]
Others	11	[43, 45, 47, 48, 50, 173–178]
No Cipher Evaluation	4	[38, 52, 53, 56]

phic metrics, while others rely predominantly on statistical visualization techniques without providing formal security analysis. In some cases, cipher implementations are not evaluated at all, especially in studies focused exclusively on the construction of chaotic S-Boxes. This heterogeneity complicates direct comparison among proposals and limits reproducibility and benchmarking consistency across different implementations and application domains.

In fact, the absence of standardized evaluation methodologies constitutes a gap identified in this SLR, representing a recommendation for future research. The metric frequencies presented in Tables 3.4 and 3.5 may contribute toward the establishment of more consistent and comprehensive evaluation practices in future studies.

3.3.3.3 Methodological Limitations in Chaos-Based Cryptography

Section 3.3.3.2 addresses not only the technical description of the solutions investigated in this SLR, but also the technical limitations of the chaos-based crypto-

graphic designs identified in the literature. These limitations cover the range of the four dimensions investigated in the technical analysis: limitations regarding the application of chaos theory (Section 3.3.3.2.1), such as the neglect of transient time (T_T) and keyspace (K_S) analysis based on valid chaotic initial conditions; limitations in the S-Boxes cryptographic primitives (Section 3.3.3.2.2), including the limited exploration of on-the-fly (*OtF*) chaotic computation approaches; limitations in the implementation of the cryptographic solutions (Section 3.3.3.2.3), particularly the scarcity of FPGA- and ASIC-oriented implementations; and limitations regarding the evaluation metrics employed (Section 3.3.3.2.4), including the absence of standardized evaluation frameworks and consistent benchmarking practices. In contrast, this Section 3.3.3.3 explicitly focuses on methodological limitations related to evaluation design, experimental validation, and the absence of formal cryptographic analysis frameworks in the primary studies.

A first limitation observed in the analyzed literature concerns the lack of a consistent and well-founded taxonomy for chaos-based cryptographic designs across primary studies. In most cases, the categorization schemes adopted in the literature are based on non-standard criteria defined by the authors, rather than being grounded in a shared and standardized conceptual framework. As a result, studies are classified using heterogeneous criteria, including chronological order of publication, intended application domains, or underlying cryptographic or chaotic mechanisms. This variability reflects subjective organizational choices rather than systematic methodological principles. Consequently, the absence of a unified taxonomic framework hinders meaningful comparison between approaches and complicates the synthesis and interpretation of results within the field. From a systematic review perspective, this inconsistency introduces an additional layer of structural heterogeneity that limits the ability to establish a coherent and consolidated view of chaos-based cryptographic research.

Other methodological limitations identified in the studies selected in this SLR concern the lack of scientific reproducibility and experimental transparency. In several studies, the source code associated with the proposed cryptographic schemes is not publicly available, even for implementations developed in MATLAB or other software-based simulation environments. Moreover, critical experimental details

such as chaotic initial conditions, and control parameters are often incompletely specified, which hinders independent reproduction and validation of the reported results. The absence of standardized reporting practices for finite-precision arithmetic and hardware-related constraints further limits the rigorous assessment of chaos degradation effects in digital implementations. In addition, hardware configurations, computational environments, and implementation-level parameters are frequently only partially described, thereby reducing experimental reproducibility, weakening benchmarking consistency, and limiting meaningful comparative analysis across different studies.

Another important methodological limitation identified in the reviewed studies concerns the absence of formally defined threat models and adversarial assumptions. Most of the analyzed works do not explicitly specify the attacker capabilities or security objectives considered during the evaluation process. In particular, there is frequently no distinction between adversarial models such as known-plaintext attacks (KPA), chosen-plaintext attacks (CPA), and chosen-ciphertext attacks (CCA). As a result, cryptographic evaluations are often conducted without a formally established security framework, relying predominantly on statistical analyses and empirical observations rather than adversarial validation under well-defined attack scenarios. This limitation is critical in cryptography, since security cannot be properly assessed without a clearly specified threat model. In practice, cryptanalytic evaluation is typically performed by independent researchers and specialized groups after publication, as cryptanalysis requires a distinct skill set from cryptographic design. Consequently, the absence of formal adversarial assumptions and clearly defined attack scenarios compromises the interpretability, comparability, and practical security relevance of many chaos-based cryptographic proposals.

A further methodological limitation concerns the absence of formal security proofs or provable security frameworks in the analyzed studies. In most cases, cryptographic strength is inferred from empirical statistical tests and heuristic arguments, without reduction-based security proofs or formal definitions of security notions such as indistinguishability under standard cryptographic models. This lack of formal validation limits the theoretical rigor of chaos-based cryptographic constructions and weakens their alignment with established cryptographic standards.

Overall, the identified methodological limitations suggest that the evaluation of chaos-based cryptographic systems is driven by empirical validation and heuristic analysis, and also shows heterogeneous alignment with established cryptographic evaluation frameworks. Similar limitations may also be observed in other cryptographic paradigms; however, their prevalence is particularly pronounced in chaos-based approaches. This lack of formal rigor affects both the methodological quality and the security assurance of the proposed schemes.

3.3.3.4 Identified Research Gaps

Beyond summarizing the current SOTA, a SLR plays a fundamental role in identifying unresolved challenges, methodological weaknesses, insufficient validation practices, and underexplored research problems, thereby supporting scientifically relevant future research directions and contributing to the advancement of the scientific knowledge frontier, as discussed in the systematic review guidelines presented in [138]. In this context, the research gaps discussed in this section were identified through the comparative and methodological analysis of the primary studies included in this SLR, particularly through recurring limitations, inconsistencies, and underexplored problems observed throughout the reviewed literature. Accordingly, the primary objective of this section is to identify the open problems and structural limitations that remain insufficiently addressed in the current SOTA of chaos-based cryptography.

Most of the analyzed studies concentrate on image encryption applications, and the majority of the identified research gaps are also associated with this domain, generally involving incremental or application-specific improvements. Although this highlights the maturity and widespread adoption of chaos-based image encryption, it also reveals a limited diversification of chaotic approaches toward broader cryptographic applications.

Recent developments in chaos-based cryptographic systems indicate that emerging research directions are increasingly oriented toward hybrid encryption paradigms that combine chaotic dynamics with complementary techniques. As evidenced by several studies in the SOTA, such as [50, 173], the integration of hyperchaotic systems with DNA cryptographic operations has been shown to enhance

nonlinear confusion and statistical diffusion properties. Similarly, hybrid constructions combining chaotic maps with algebraic structures, genetic algorithms, and probabilistic coding schemes [38, 43] further demonstrate that the combination of heterogeneous mechanisms can significantly improve resistance to cryptanalytic attacks while expanding the effective design space of cryptographic primitives. Overall, the SOTA suggests that future advancements in chaos-based cryptography are likely to converge toward hybrid cryptographic frameworks that systematically combine chaos theory with bio-inspired, algebraic, and stochastic techniques.

The analysis of the reviewed studies reveals a significant gap between algorithmic design and practical implementation. The majority of the proposed chaos-based cryptographic systems are developed and validated primarily through software-based simulations, typically using environments such as MATLAB or similar numerical platforms. In contrast, hardware-oriented implementations, including FPGA and SoC architectures, remain relatively scarce and are often not designed with explicit consideration of architectural constraints such as area, latency, power consumption, and finite-precision effects. This indicates a persistent gap between theoretical cryptographic constructions and their practical deployment in real-world embedded and hardware-constrained environments.

In addition, the generation of chaotic sequences in the reviewed literature is predominantly performed offline, with most studies relying on precomputed values stored in S-Boxes or LUTs. This design choice simplifies algorithmic validation but limits the dynamic nature of chaos-based cryptographic systems. The limited adoption of OtF (online) chaotic sequence generation highlights an important open research direction, particularly in the context of hardware-efficient, cipher security, and dynamically reconfigurable cryptographic architectures, where real-time generation of chaotic states may improve both security robustness and adaptability.

Another research gap identified in the analyzed literature concerns the absence of standardized methodologies and unified evaluation frameworks for assessing the cryptographic quality of S-Boxes. Although many primary studies employ classical evaluation metrics such as nonlinearity, bijectivity, differential uniformity, SAC, and BIC, the selection and reporting of these metrics remain insufficiently standardized across the literature. In many cases, the evaluation process is limited to a subset

of properties, preventing fair and reproducible comparisons among different S-Box designs. Furthermore, the lack of standardized benchmarking criteria, including clearly defined relative weighting schemes and consolidated scoring methodologies, limits the establishment of universally accepted quality thresholds for the evaluation of chaos-based S-Boxes.

Beyond the evaluation of S-Boxes, a complementary research gap is observed at the cipher level, where the evaluation of chaos-based cryptographic algorithms as complete encryption systems also lacks methodological standardization. Although established evaluation frameworks exist, such as NIST statistical test suites, none of the literature included in this SLR employs a uniform and standardized framework to evaluate cipher strength. As a result, performance and security claims are supported by fragmented or application-specific evaluations, without systematic comparison against a predefined set of established cryptographic benchmarks. In addition, standardized reference algorithms such as AES could serve as baseline models for comparative evaluation, enabling more rigorous assessments of diffusion, confusion, computational efficiency, and resistance to cryptanalytic attacks. However, such comparative approaches remain underutilized in the literature, limiting the ability to objectively position chaos-based ciphers within the broader landscape of established cryptographic systems.

Furthermore, within a unified evaluation framework for both cryptographic ciphers and S-Boxes, defined by a structured set of metrics with associated weighting schemes, chaos-based cryptographic algorithms must include additional metrics related to the quality of the underlying chaotic systems or maps. In the absence of such considerations, there is a risk that the cipher operates outside the valid dynamical specifications of the chaotic model, potentially invalidating the assumed cryptographic properties. In particular, the evaluation should explicitly account for characteristics such as the valid region of initial conditions, chaotic keyspace (K_S) analysis, transient time (T_T), dispersion time effects, and chaos degradation effects. These aspects are introduced in Section 3.3.2.1 and are fundamental to ensuring that the chaotic system preserves its intended behavior under numerical discretization and hardware implementation constraints. Without incorporating these criteria into the evaluation framework, the resulting assessment may overestimate the

cryptographic strength of chaos-based constructions and fail to detect structural vulnerabilities introduced by improper chaotic regime selection.

Therefore, an important research gap concerns the insufficient verification of whether the chaotic systems employed in cryptographic algorithms effectively preserve their chaotic behavior after numerical discretization, finite-precision implementation, and integration into practical digital architectures. In many studies, chaotic properties are assumed rather than systematically validated throughout the encryption process. However, implementation-related effects such as finite numerical precision, transient dynamics, parameter deviations, and chaos degradation may significantly alter the original dynamical behavior of the system, potentially reducing unpredictability and weakening cryptographic security. Consequently, several chaos-based cryptographic schemes may operate outside the intended chaotic regime without explicit detection, highlighting the necessity of incorporating dynamical-system validation procedures into future cryptographic evaluation methodologies.

Collectively, these identified gaps emphasize the need for more rigorous, implementation-aware, and theoretically grounded evaluation frameworks for chaos-based cryptographic systems. In particular, future research should systematically integrate algorithmic design, standardized cryptographic benchmarking, and dynamical-system validation to ensure consistency between theoretical chaotic models and their practical cryptographic realizations.

3.3.3.5 Positioning of This Work

This work presents two primary contributions derived from the structured analysis conducted in Chapter 3. First, the Survey of Surveys (SoS) presented in Section 3.2 reveals a clear gap (Section 3.2.3) in the literature, namely the absence of dedicated surveys focusing on chaos-based S-Box designs. This gap motivates the development of a systematic literature review (SLR), which constitutes the first contribution of this thesis and is presented in Section 3.3. The SLR establishes a focused and structured characterization of chaos-based cryptographic designs, with particular emphasis on S-Boxes, and provides a consolidated view of the current state of the art (SOTA). This first contribution, of methodological nature, establishes the analytical and scientific foundation of the thesis by providing a structured and

comprehensive characterization of the current SOTA in chaos-based S-Box research.

The proposed research is positioned within the emerging transition from static and software-oriented chaos-based cryptographic constructions toward dynamically reconfigurable and implementation-aware architectures. While a significant portion of the current literature relies on offline generation mechanisms, pre-computed lookup structures, and software-based validation environments, the approach developed in this thesis emphasizes runtime adaptability through OtF chaotic computation and dynamically generated chaos-based S-Boxes. Furthermore, unlike many existing proposals that primarily focus on statistical validation for image encryption applications, the present work incorporates broader cryptographic and implementation-oriented considerations, including dynamical-system validation, finite-precision effects, architectural feasibility, and hardware-oriented constraints. Consequently, this research positions itself at the intersection of nonlinear dynamical systems, cryptographic primitive design, and hardware-aware cryptographic architectures.

Second, the systematic analysis performed in the SLR leads to the identification of several fundamental gaps, as discussed in Section 3.3.3.4. These gaps motivate the second contribution of this work, namely the design and evaluation of a chaos-based S-Box construction employing OtF computation strategies, which directly addresses limitations related to static precomputation and lack of dynamical adaptability observed in the literature. This technical and experimental contribution is developed in Chapter 5, where its effectiveness is assessed in terms of cryptographic performance, security, and implementation considerations.

Therefore, this thesis contributes not only to the consolidation of the current SOTA through a dedicated SLR on chaos-based S-Boxes, but also to the advancement of the field through the proposal of a dynamically generated chaos-based cryptographic structure designed to address several of the methodological and architectural limitations identified throughout the reviewed literature. By integrating OtF chaotic computation, dynamic S-Box generation, and implementation-aware design considerations, the proposed approach seeks to advance the development of more adaptable, and practically deployable chaos-based cryptographic systems.

3.3.3.6 Threats to Validity and Limitations

This section discusses the threats to validity and methodological limitations associated with the two review processes conducted in this chapter, with primary emphasis on the Systematic Literature Review (SLR) presented in Section 3.3. The Survey of Surveys (SoS), presented in Section 3.2, is considered in a complementary and contextual manner, as its limitations are primarily circumstantial and related to its role in supporting the definition and positioning of the SLR described in Section 3.3. Although both reviews were conducted following structured and systematic procedures, limitations and potential sources of bias are inherent to literature review methodologies. Explicitly acknowledging these limitations not only increases the scientific credibility of this SLR, but also identifies opportunities for methodological refinement and future research directions in subsequent SLRs.

3.3.3.6.1 Limitations of the Survey of Surveys

The Survey of Surveys (SoS) conducted in Section 3.2 is subject to limitations that are common to secondary studies in the field of systematic literature analysis. Although a structured protocol was followed, supported by the Parsifal online platform (<https://parsif.al/>), including the use of the PICOC framework and multiple digital databases, the completeness and coverage of the retrieved corpus remain dependent on the limitations and potential sources of bias discussed in this section.

An identified limitation is related to the selection and screening process, which inherently involves a degree of subjectivity, particularly during title and abstract screening, as well as during the application of the inclusion and exclusion criteria. Despite the use of predefined criteria and the support provided by the Parsifal tool, interpretation bias may still influence the final set of included studies. For instance, a poorly descriptive title may discourage or prevent the inspection of the corresponding abstract, potentially leading to the exclusion of relevant studies without a subsequent full-text analysis. To mitigate this threat, reassessment procedures and secondary inspections of excluded studies may be performed after each screening phase in order to reduce the likelihood of premature exclusions, or even forcing a study into a deeper analysis in the next screening phase in order to ensure

completeness (as illustrated in the following examples [184–186]). In addition, the quality assessment process, although based on explicit scoring criteria, still involves weighting decisions that may affect the classification and retention of borderline studies. Consequently, changes to the minimum quality score threshold could result in the inclusion of additional studies in the SoS.

Another relevant threat to validity concerns the heterogeneity of the included studies, which vary significantly in scope, methodology, and application domain. While this diversity enables a broader synthesis of the literature, it limits the extent to which direct quantitative comparisons can be established and may introduce interpretative bias during synthesis and classification. In addition, the findings of this SoS are affected by temporal and publication biases, given that chaos-based cryptography is a rapidly evolving field. Despite these limitations, the SoS provides a structured overview of existing literature reviews and supports the development of the systematic literature review presented in this chapter.

3.3.3.6.2 Limitations of the Systematic Literature Review

The Systematic Literature Review (SLR) conducted in Section 3.3 is subject to inherent limitations and threats to validity commonly associated with systematic review methodologies. Similarly to the SoS case conducted in Section 3.2, this study also is supported by the Parsifal online platform, including the PICOC framework. However, in the case of the SLR, the analysis is further constrained by its dependence on primary studies, whose reported results, experimental settings, and evaluation metrics may vary significantly across contributions. As a result, the completeness, consistency, and comparability of the extracted evidence remain subject to the methodological constraints and potential sources of bias discussed in this section.

The planning phase of the SLR is directly derived from the research gap identified in the preceding SoS, which motivated the focus on chaos-based cryptographic systems, with emphasis on S-Boxes design. In this context, the PICOC formulation intentionally establishes S-Boxes as the central analytical construct, reflecting the specific objective of the study rather than an unrestricted exploration of chaos-based cryptography. While this explicit scoping is necessary to implement the review and ensure methodological traceability with respect to the identified research gap, it

also implies a deliberate narrowing of the analytical universe, in which studies that employ chaotic systems in cryptographic contexts without explicit S-Boxes formulation may not be fully captured. This includes, for instance, works focusing on chaos-driven key generation, permutation-diffusion architectures, or hybrid cryptographic primitives in which S-Boxes design is implicit rather than explicitly defined, and which are intentionally not part of this SLR.

The search string is the first implementation of the scoping decisions defined in the planning phase of the SLR, translating the conceptual focus on S-Boxes into a structured query formulation. In this context, the Boolean expression combines terms related to S-Boxes, chaos theory, and cryptographic properties in order to maximize the retrieval of studies aligned with the target construct. However, this translation from conceptual scope to executable query introduces a measurable source of selection bias, as the effectiveness of the search process becomes directly dependent on synonym coverage, terminology alignment, and available selection tools within the databases. Consequently, studies that describe equivalent concepts using alternative formulations, such as chaos-based permutation mechanisms or implicit substitution structures, are intentionally excluded from this SLR and may remain outside the retrieved corpus.

The selection criteria operate on the extracted set of studies through the search string and translate the predefined search scope into explicit inclusion and exclusion decisions. In this phase, studies are primarily assessed based on the information available mainly in the title and keywords, with the abstract used as a secondary filter when necessary, creating a dependency on the completeness and accuracy of these elements for proper classification. Although this approach supports a systematic screening process, it introduces a potential bias, since relevant studies may be excluded when important methodological details are not explicitly described in these parts of the study metadata, even if they are present in the full text. To reduce the risk of premature exclusion, some borderline studies were retained for quality assessment despite weak initial screening signals, as exemplified by [187–189], which advanced to the next screening stage but were later discarded.

The quality assessment checklist introduces an additional layer of structured evaluation. In this phase, the assessment is primarily based on the presence of ex-

plicit information related to research objectives, contributions, cryptographic primitives, chaotic systems, security, performance, and publication in peer-reviewed journals, using the abstract as the primary basis of analysis and consulting the full text when necessary. Although this approach supports standardization, it may introduce evaluation bias, since the perceived quality of a study may depend more on the completeness of its abstract than on the actual methodological rigor of the study itself. Furthermore, the grading structure and cutoff score adopted reduce complex methodological characteristics into discrete evaluation levels, which may limit the analysis of borderline studies. To reduce this limitation, full-text inspection was performed whenever the abstract-level assessment was insufficient to support the classification. Similarly, some borderline studies were retained for data extraction despite ambiguous assessment signals, as exemplified by [190, 191], which were ultimately not included in the final list presented in Table 3.2.

The data extraction form was designed to standardize the collection of bibliographic, bibliometric, cryptographic, implementation, and evaluation-related information from the selected studies, enabling structured comparison across different approaches. Although this strategy improves traceability and facilitates systematic analysis, it may introduce data abstraction bias, since heterogeneous methodologies, evaluation procedures, and architectures must be mapped into predefined extraction categories. In this context, complex or partially reported characteristics, such as chaos degradation effects, transient-time computation, hybrid designs, or implementation details, may be inconsistently described across studies, making accurate classification dependent on interpretation. Furthermore, several extracted attributes rely on self-reported experimental results provided by the authors, which may not follow directly comparable testing conditions. Consequently, the extracted data may reflect variations arising not only from differences in the cryptographic approaches, but also from inconsistencies in reporting practices, experimental configurations, and evaluation criteria adopted. The implementation of all designs presented in Table 3.2 was considered out of scope for this SLR, being left as a suggested future work.

The SLR is subject to a limitation of semantic non-equivalence and heterogeneity across the included studies. In the context of chaos-based S-Boxes,

different works evaluate distinct constructs under the same objective of evaluating S-Box quality, relying on heterogeneous validation criteria, including statistical randomness tests, cryptographic structural metrics, and application-specific image encryption measures. In addition, these studies are often designed for different application domains, such as multimedia encryption [42–46], telecommunication [56,174], or hardware-oriented implementations [53]. Although the SLR adopts a unified analytical framework, this heterogeneity in both evaluation criteria and application objectives leads to the aggregation of non-comparable experimental targets and introduces a task-dependent bias in the synthesis process. This limitation is inherent to the nature of the primary studies and lies outside the scope of this SLR, which does not attempt to normalize or re-define the underlying evaluation criteria across different works.

The SLR is affected by reproducibility constraints arising from incomplete reporting and limited availability of experimental artifacts in the primary literature. Many included studies do not fully disclose implementation details, chaotic parameter configurations, or source code, which hinders independent replication of results. This lack of reproducibility introduces a secondary layer of uncertainty into the synthesis process, as the SLR must rely on potentially non-verifiable empirical claims, thereby limiting independent verification and replication of the reported results.

A further methodological limitation concerns the use of evaluation metrics originally designed for conventional cryptographic primitives in the context of chaos-based S-Boxess. Commonly adopted measures such as NIST statistical test suites, nonlinearity (NL), avalanche-related criteria, and image-based metrics such as NPCR and UACI are frequently employed as indicators of cryptographic strength without explicit validation of their construct validity in chaotic encryption. This reliance on inherited metrics introduces a threat to validity, as these measures may not fully capture relevant properties of dynamically generated chaotic systems, as discussed in Section 3.3.2.1 and in [4]. In addition, the absence of a well-defined cryptographic equivalence framework for chaos-based S-Boxess prevents the establishment of a consistent basis for comparing different constructions, as there is no universally accepted criterion for determining equivalent security strength or resistance to cryptanalytic attacks. Nevertheless, the development of a dedicated metric

evaluation framework specifically tailored to chaos-based S-Boxess and chaos-based cryptography lies outside the scope of this SLR.

3.4 Chapter Conclusions

Based on a research gap identified through a Survey of Surveys (SoS), this Systematic Literature Review (SLR) examines the intersection between chaos theory and cryptography, with emphasis on the design and application of chaos-based cryptographic systems employing substitution boxes (S-Boxes). Across the surveyed literature, chaotic systems are consistently associated with properties such as sensitivity to initial conditions and ergodicity, which are commonly related to the cryptographic principles of confusion and diffusion. Early pioneering studies established the feasibility of integrating chaotic maps into encryption schemes, forming the conceptual basis for subsequent developments in chaos-based cryptography.

The state-of-the-art (SOTA) in chaos-based S-Boxes is characterized by a wide variety of construction strategies, ranging from one-dimensional and multi-dimensional chaotic maps to hybrid formulations combining algebraic structures, genetic algorithms, quantum random walks, and alternative mathematical constructs. Despite this diversity, the literature converges on the use of dynamic and key-dependent S-Boxes as mechanisms intended to improve statistical and structural cryptographic properties, including nonlinearity (NL), bijectivity, avalanche behavior, and resistance to classical differential and linear cryptanalysis when compared to static constructions.

Despite significant advances, several challenges remain. Many studies do not fully address the impact of initial conditions that may drive chaotic maps into non-chaotic regimes, potentially weakening security. The transient behavior of chaotic systems, chaos degradation under finite-precision implementations, and the lack of hardware-oriented analyses in some approaches also constitute obstacles for practical deployment. Furthermore, few works evaluate performance in resource-constrained or real-time scenarios, highlighting opportunities for future FPGA- and ASIC-based implementations. In addition, evaluation practices frequently rely on heterogeneous criteria, which limits the direct comparability of results across different proposals

and application domains, particularly in contexts such as multimedia encryption and resource-constrained implementations.

The conducted SLR indicates that chaos-based cryptography, particularly the generation of dynamic S-Boxes, remains an active research direction for the development of adaptive encryption systems. Future research should focus on rigorous analysis of initial condition selection, mitigation of chaos degradation effects, efficient hardware-oriented implementations, hybrid designs, and the evaluation of multi-parameter hyperchaotic systems under standardized validation criteria. In addition, further investigation is required to reduce the dependence on application-specific assumptions and predominantly empirical validation practices currently observed in the literature. Addressing these challenges may contribute to improving the consistency, reproducibility, and practical applicability of chaos-based cryptographic systems.

In conclusion, chaos-based cryptography remains a relevant research direction for the construction of dynamic substitution mechanisms and adaptive encryption architectures. Nevertheless, the transition from predominantly simulation-based studies to reproducible and deployment-oriented cryptographic systems is still constrained by the absence of standardized evaluation criteria, consistent benchmarking methodologies, and validation approaches accounting for hardware and finite-precision effects.

Chapter 4

Materials and Methods

From Concept to Implementation: The Path of Scientific Construction

4.1 Materials

Regarding the materials used in this thesis, the following hardware and software resources were employed in the present research: a Lenovo ThinkPad E14 Gen2 computer manufactured in Brazil, equipped with an 11th Generation Intel® Core™ i5-1135G7 @ 2.40 GHz processor (base frequency 2.42 GHz), featuring four physical and eight logical *Central Processing Units* (CPUs), 8 GB of RAM, and 128 MB of video memory. The system operated under Windows 11 Pro 64-bit, version 22H2.

This hardware configuration was selected based on the working conditions available in the laboratory. These specifications provided sufficient processing power to handle the synthesis and simulation workloads associated with the proposed cryptographic architecture, including tasks involving high-level modeling and bitstream generation. The use of an available commercial-grade laptop enhances the reproducibility of the experiments, ensuring that all results can be replicated on comparable platforms without reliance on specialized or high-end computing infrastructure.

A virtual machine was also employed with the following specifications: Oracle VM VirtualBox 7.0 (build 7.0.18 r162988), configured with 2 GB of RAM

allocated from the 8 GB available on the host system, 32 MB of video memory from the 128 MB available, and two CPU cores from the eight logical cores of the host. The virtual machine executed the following software stack: Windows XP (32-bit), version 5.1, build 2600, Service Pack 1 as the operating system; MATLAB version 6.5.0.180913a (Release 13); Xilinx ISE Design Suite v12 (P/N 1050504-01) with Xilinx Project Navigator v6.2i; Xilinx System Generator Blockset v6.1(c); and ModelSim XE 6.2i.



Figure 4.1: Software package

This virtualized environment was adopted to mitigate compatibility issues associated with legacy software tools available in the laboratory and designed for 32-bit operating systems. By encapsulating the software stack within a controlled virtual environment, the setup ensured the stable and consistent execution of all toolchains required throughout the modeling, simulation, and synthesis stages of the proposed cryptographic architecture. The use of VirtualBox offered significant portability advantages, allowing the same configuration to be easily replicated across different host machines, consequently enhancing the reproducibility of experiments

for future researchers under comparable conditions.

A Xilinx Spartan-3 development board, manufactured by Avnet in the United States (P/N ADS-XLX-SP3-DEV2000), was also utilized in this research. The board's main components include a Xilinx XC3S1500/2000-FG676 Spartan-3 FPGA, 43 MB Micron *Double Data Rate* (DDR) *Synchronous Dynamic Random-Access Memory* (SDRAM), 16 MB Flash memory, 2 MB *Static Random-Access Memory* (SRAM), a 2×16 *Liquid Crystal Display* (LCD), a 128×64 OSRAM *Organic Light-Emitting Diode* (OLED) display, and an integrated audio codec. This development platform was selected among those available in the laboratory due to its flexibility and suitability for implementing and testing digital circuits in hardware. The board provided sufficient resources to support the design, synthesis, and evaluation of the proposed CB-SBox.

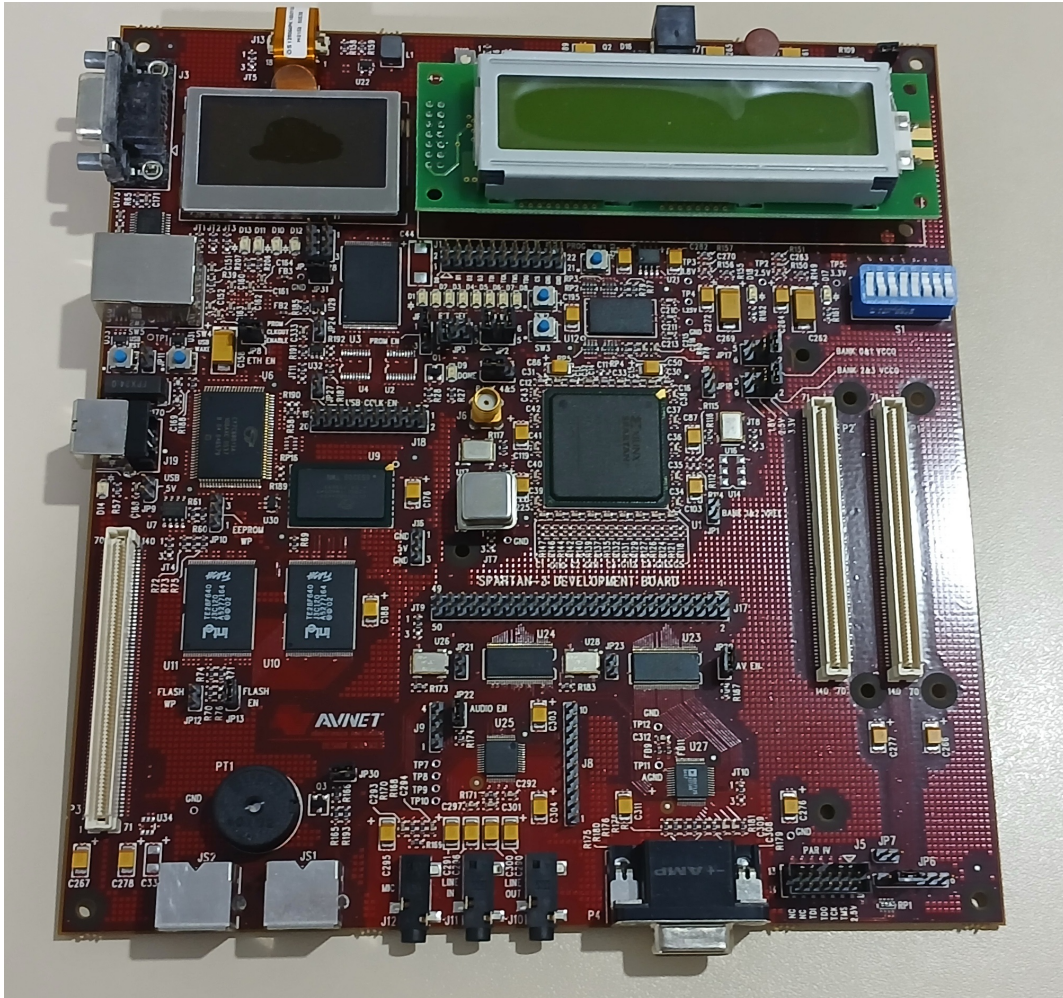


Figure 4.2: Xilinx Spartan-3 development board



Figure 4.3: Power and data cables used in a Xilinx Spartan-3 development setup

4.2 Methods

The methodological workflow adopted in this thesis comprised four main stages, as briefly explained in the following paragraphs.

First, based on an exploratory SoS, which identifies research gaps in structured surveys covering the use of chaos-based S-Boxes in cryptography, a SLR was conducted to define and characterize the primary contribution of this work (see Chapter 3): the use of chaos for the development of an on-the-fly S-Box intended for application in block ciphers.

Second, based on the method proposed in [4], which employs a metric consisting of four quantitative parameters (Attractor Density, Largest Subset Volume, Distance-to-Time Ratio, and Maximum Dispersion Time) and a weighted grading scheme, six chaotic systems (among a universe of more than 40 existing ones) were modeled in MATLAB to analyze their numerical behavior, ergodicity, and discretization accuracy under finite-word-length constraints (see Section 5.2), with the aim of selecting the most suitable system for cryptographic applications, particularly for the proposed CB-SBox (see Section 5.3).

Third, based on the chaotic system selected using the method proposed in [4], the digital implementation of the proposed CB-SBox was synthesized using the Xilinx System Generator Blockset v6.1(c) software (see Section 5.3), employing a multi-rate strategy and a configurable database. The proposed CB-SBox was analyzed in terms of area and power consumption, timing performance, security (considering linear and differential resistance to cryptanalysis), and bijectivity.

Finally, the designed CB-SBox was integrated into a Feistel network based on [24], and the validated architecture was implemented targeting the Xilinx Spartan-3 development FPGA board. Performance metrics, including maximum operating frequency, data rate, FPGA resource utilization, and circuit cost, were measured with respect to the number of bits employed in the CB-SBox. The resulting block cipher was applied to image and text encryption and statistically analyzed using histogram techniques.



Figure 4.4: Experimental setup used for the design, simulation, and validation of the proposed solution.

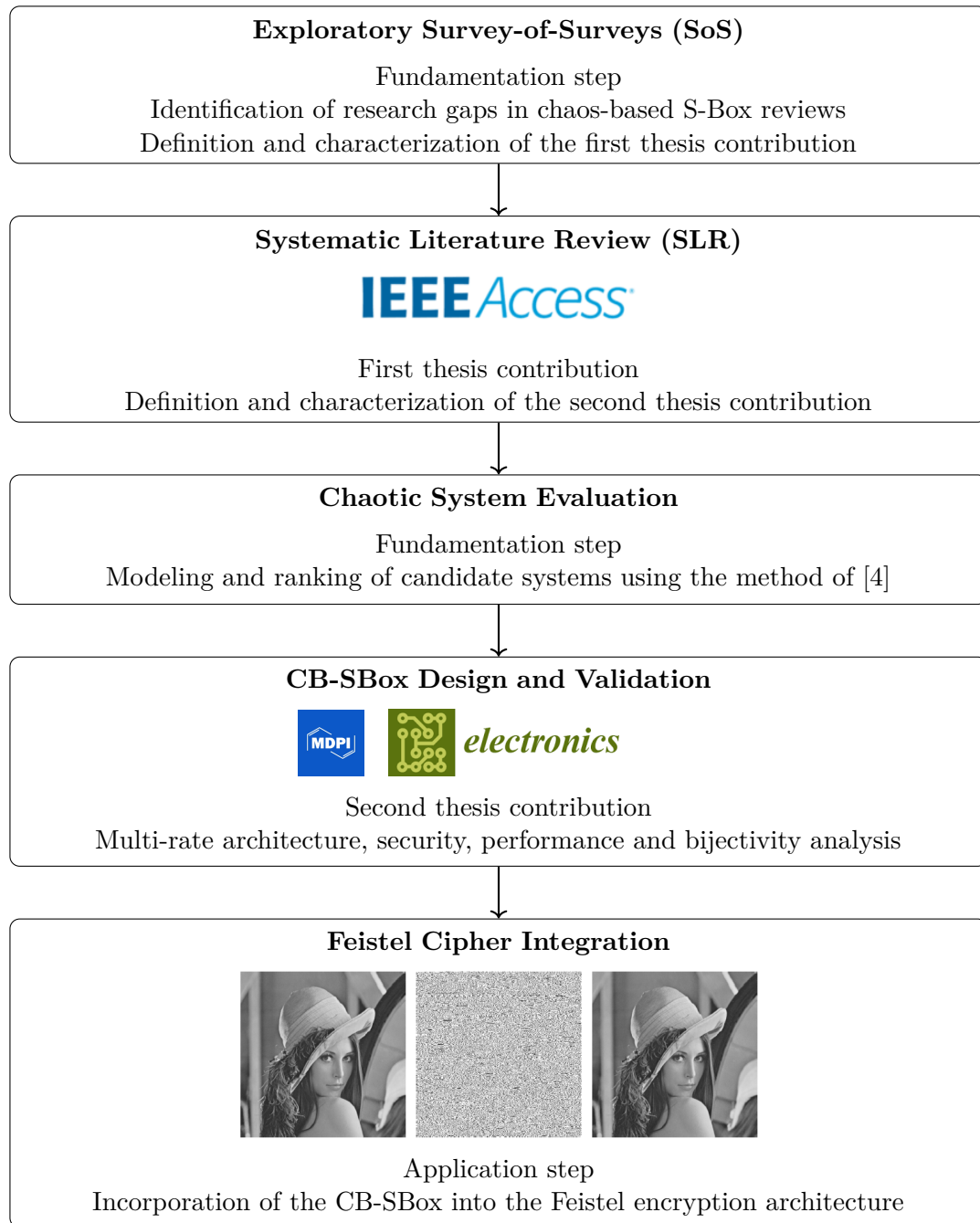


Figure 4.5: Methodological workflow adopted in the research.

Chapter 5

Experimental Results

Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives

5.1 Chapter Introduction - CB-SBox

Since Lorenz’s 1963 seminal article [6], more than forty non-linear differential equations presenting chaotic behavior have been reported [1, 7–11]. They have been applied to many disciplines, including cryptography [23–39, 41–61]. Chaos and encryption are intimately tied: confusion and diffusion, two fundamental concepts of cryptography [62], are strongly related to the chaotic properties of ergodicity and sensitivity to ICs [63]. This relation led many researchers to develop chaos-based encryption algorithms. Many of these developed chaos-based encryption algorithms use chaos for constructing or populating tables and S-Boxes. In parallel, some studies investigated the conditions for applying chaos theory in encryption. The behavior of chaotic maps is highly sensitive to variations in ICs, and in some cases, chaotic behavior may even vanish for specific ICs values, causing the map to either converge to a fixed point or diverge away from the attractor.

The main contribution of this work is to propose an S-Box implementation in which traditional LUT structures are replaced by an OtF fixed-point arithmetic calculation of a non-linear differential equation. This structure is referred to as a CB-SBox and offers notable advantages in terms of area, power consumption, and cryptographic strength. Its temporal evolution drives the initial state x_0 , also re-

ferred to as the initial condition (IC), toward a deterministically linked yet uncorrelated final state x_f . The final state is reached after executing the chaotic map for a fixed number of iterations. To the best of the authors' knowledge, this is the first attempt to design a chaotic S-Box based on this OtF approach.

The rest of this chapter is organized as follows: Section 5.2 discusses the fixed-point arithmetic implementation of six non-linear differential chaotic maps. The evaluation method proposed in [4] is applied to select a chaotic map suitable for a Chaos-Based Substitution Box. In Section 5.3, the chosen map is used to construct a Chaos-Based Substitution Box (CB-SBox) circuit. This construction allows the final state of the selected differential chaotic map (the circuit output) to be obtained by feeding an initial condition into the circuit's input. Section 5.4 compares the properties of the proposed CB-SBox with a typical memory-based LUT implementation. For a fair comparison, both implementations are carried out on an ASIC using *VHSIC Hardware Description Language* (VHDL). Parameters such as power, area, and time are analyzed in this section. The security improvements are evaluated by measuring resistance to differential and linear cryptanalysis [192]. Based on the proposed CB-SBox and the design decisions from the previous sections, Section 5.5 presents an application of the CB-SBox in a Feistel network block cipher from [24]. Finally, Section 5.6 concludes the article by summarizing the results and providing a glimpse of future work.

5.2 Chaotic Map Evaluation

The S-Box proposed in this work is referred to as the CB-SBox. Its core is the fixed-point implementation of a non-linear differential system exhibiting chaotic behavior. From a collection of more than forty existing chaotic maps and systems [1, 7–11], six were selected and evaluated using the method proposed in [4], with the objective of identifying the most suitable candidate for the CB-SBox design. The evaluation set was limited to six maps due to the significant computational effort required to simulate the evolving states driven by different ICs across the allowable state space. Notably, the evaluation included the Sprott N map instead of the Sprott A, which demonstrated poor Attractor Density (d_A) values [4], and the plate

39 configuration was preserved for Chua's map.

The evaluation method described in [4] tracks four quantitative parameters (see Table 5.1): Attractor Density ($d_{\mathcal{A}}$), Largest Subset Volume (V_{Sub}), Distance-to-Time Ratio (DTR), and Maximum Dispersion Time (MDT). The first parameter, Attractor Density ($d_{\mathcal{A}}$), directly reflects the spatial distribution of a strange attractor *Strange Attractor* ($\mathcal{A}$) [193]: the set of states in the state space of a chaotic map. Low values of *Attractor Density* ($d_{\mathcal{A}}$) indicate that the chaotic map has poor dispersion capability across the state space, which is typically undesirable in applications such as chaotic encryption, where performance relies on the butterfly effect [96]. Let $BP_{\mathcal{A}}$ be the smallest axis-aligned bounding parallelepiped that contains the set $\mathcal{A}$, and suppose it is partitioned into smaller parallelepiped volumes sp . Let $Vol(\cdot)$ denote the volume function. If k of these sub-volumes contain at least one point of $\mathcal{A}$, then the $d_{\mathcal{A}}$ is calculated as follows in Equation (5.1):

$$d_{\mathcal{A}} = \lim_{Vol(sp) \rightarrow 0} \left(\frac{\sum_{n=1}^k Vol(sp_n)}{Vol(BP_{\mathcal{A}})} \right) \quad (5.1)$$

The second parameter, obtained from [4], the *Largest Subset Volume* (V_{Sub}), is the subset volume that can be extracted from *Volume of Valid Initial Conditions* (V_{IC}) (the three-dimensional volume containing all ICs capable of originating a strange attractor $\mathcal{A}$ as shown in Figure 5.1). Let $|\cdot|$ be the cardinality function, let $[\cdot]^c$ denote the complement operation between sets, let $\cup$ be the union operator, let SS be the set of ICs belonging to the state space, let $\mathcal{A}_{all}$ be the set of all possible attractors of a chaotic map, and let $\mathcal{A}_{cv}$ and $\mathcal{A}_{dv}$ be, respectively, the subsets of degenerated attractors that converge to a pole and those that diverge to infinity, both belonging to $\mathcal{A}_{all}$. Then, the set of strange attractors $\mathcal{A}$ is defined as $[\mathcal{A}_{cv} \cup \mathcal{A}_{dv}]^c$, and the V_{IC} is defined by Equation (5.2):

$$V_{IC} = \lim_{|SS| \rightarrow \infty} \left(\bigcup_{IC \rightarrow \mathcal{A}} [IC] \right) \quad (5.2)$$

The V_{IC} of each chaotic system has an irregular shape, which is difficult to represent analytically, and is best visualized graphically (see Figure 5.1). To overcome this intractability, the V_{Sub} is defined as the volume of the largest parallelepiped entirely contained within V_{IC} . Unlike V_{IC} , the V_{Sub} has tractable orthogonal bound-

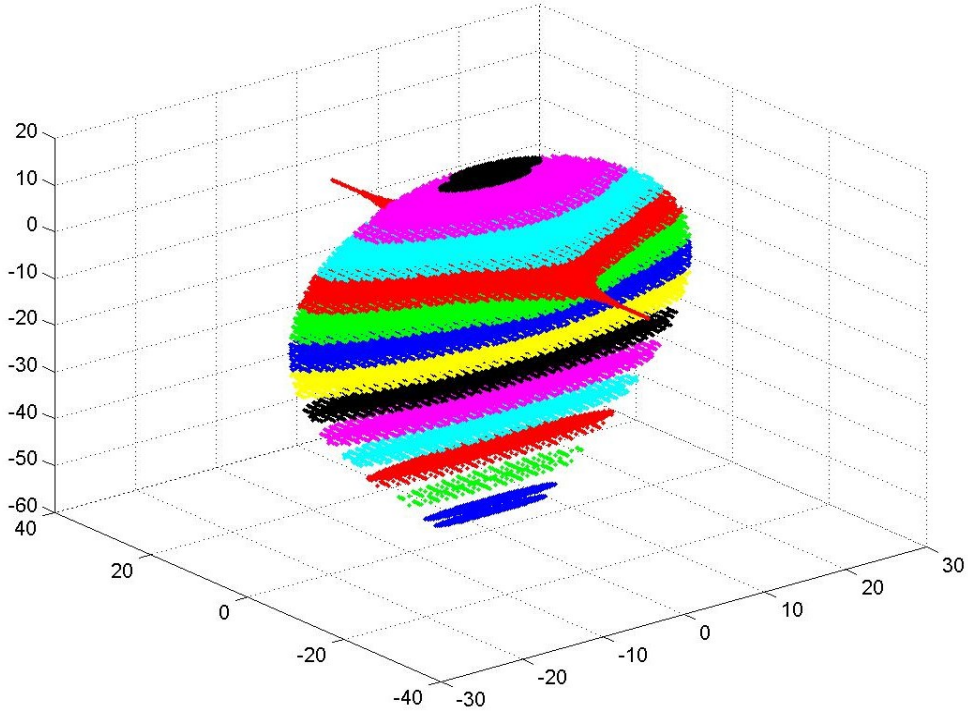


Figure 5.1: Three-dimensional V_{IC} , computed for the Sprott B chaotic map [1], adapted from [2], and made available online in [3] to support three-dimensional visualization.

aries, making it suitable for microelectronic realizations. This subset can provide a sufficient number of ICs for a wide range of applications. The use of ICs not belonging to V_{IC} leads to degenerate attractors ($\mathcal{A}_{cv}$ or $\mathcal{A}_{dv}$), which weakens chaotic maps realizations by making the map's future states predictable, an undesired effect, especially in encryption applications. Let $Var(\cdot)$ be the function that measures the maximum variation of a given variable, and let $h_{V_{IC}}$, $w_{V_{IC}}$, and $d_{V_{IC}}$ represent the three dimensions of the largest parallelepiped within V_{IC} . Then, the volume V_{Sub} is calculated by Equation (5.3):

$$V_{Sub} = Var(h_{V_{IC}}) \times Var(w_{V_{IC}}) \times Var(d_{V_{IC}}) \quad (5.3)$$

The third parameter, obtained from [4], *Distance to Time Ratio* (DTR), deals with the dispersion of the chaotic output states over $\mathcal{A}$. Let V_{Hist} be a normalized metric with $V_{Hist} \rightarrow 1$ representing a complete dispersion, let n be the number of dimensions of a chaotic map, let m be the number of output bins of a histogram

function, let B_{mn} be the m -set histogram bins measured for dimension n , and let $\min(\cdot)$ and $\text{ave}(\cdot)$ be the minimum and mean function, respectively. Then, V_{Hist} can be calculated by the product of Equation (5.4):

$$V_{Hist} = \prod_{i,j=1}^{n,m} \left(\frac{\min(B_{ji})}{\text{ave}(B_{ji})} \right) \quad (5.4)$$

Because of the butterfly effect [96], given a set of ICs and considering the *Small Distance* (ds) between neighboring ICs, after some time, the corresponding final states disperse over $\mathcal{A}$ beyond a given threshold measured by V_{Hist} . Smaller distances ds require more time to achieve this dispersion, leading to a negative ratio between ds and time. Let V_{Hist} be a given dispersion threshold, let $\text{ave}(\cdot)$ denote the mean function, let $d(\cdot)/dt$ represent the temporal derivative of a given function, and let $g(\cdot)$ be the function that relates the minimum distance ds between successive ICs to the time necessary for their outputs to spread beyond the V_{Hist} threshold. Then, the evaluation parameter DTR can be calculated by Equation (5.5). The reader should note that smaller absolute values of DTR imply that, for the same distance ds between successive ICs, less time is needed to disperse the state outputs over $\mathcal{A}$, which is a desirable property for chaotic systems:

$$DTR_{V_{Hist}} = \text{ave} \left(\frac{d(g_{V_{Hist}}(ds))}{dt} \right) \quad (5.5)$$

The fourth parameter, obtained from [4], *Maximum Dispersion Time* (MDT), also deals with the dispersion of the chaotic output states over $\mathcal{A}$. Let V_{Hist} be a given dispersion threshold, let $\max(\cdot)$ be the function that measures a maximum peak value, and let $g(\cdot)$ be the function that relates the minimum distance ds between successive ICs to the time necessary to spread the outputs over $\mathcal{A}$, beyond the V_{Hist} dispersion threshold. Then, the evaluation parameter MDT can be calculated by Equation (5.6):

$$MDT_{V_{Hist}} = \lim_{ds \rightarrow 0} (\max (g_{V_{Hist}}(ds))) \quad (5.6)$$

The MDT parameter represents an upper bound concerning the time necessary to disperse the output states of a given chaotic map, which does not depend on the distance ds between successive ICs. Observe that the distance ds is directly re-

lated to the Discretization Criterion adopted by the microelectronic implementation of a given chaotic map.

After calculating the four parameters $d_{\mathcal{A}}$, V_{Sub} , DTR, and MDT discussed in this section, we obtain the data presented in Table 5.1. Note that the best choice considering the Attractor Density ($d_{\mathcal{A}}$) is Sprott B, which exhibits the strongest ergodicity among the analyzed maps. Regarding V_{Sub} , the best option would be Sprott N, as it presents a larger parallelepiped volume containing the valid initial conditions (V_{IC}). The Distance-to-Time Ratio (DTR) presents negative values as expected. Sprott B is the best choice for this parameter, as it has the smallest absolute values of DTR, implying that, for the same distance ds between successive ICs, less time is required to disperse the state outputs over $\mathcal{A}$. Finally, the MDT shows that the best choice regarding this criterion is also Sprott B, which disperses its outputs over $\mathcal{A}$ the fastest. For the final conclusion, the grades in Table 5.1 are normalized, with the best score set to 1. A final score is calculated based on a set of four weights (r, s, t, u) , defined as $(0.20, 0.34, 0.12, 0.34)$. The weighted average grade is shown in the last column of Table 5.1. The evaluation method ultimately allows for the selection of the highest-scoring map, Sprott B as highlighted in Table 5.1, making it the most suitable for the intended application.

Table 5.1: Performance comparison of six selected chaotic maps according to the four-parameter evaluation method proposed in [4], available online in [3].

Equation	$d_{\mathcal{A}}$	V_{Sub}	DTR	MDT	Grade
Chua 39 [10]	0.0574	3.200×10^1	-486	8558	0.1353
Rössler [7]	0.0773	6.553×10^4	-235	8251	0.1790
Linz [11]	0.0938	2.000×10^0	-173	3610	0.2648
Sprott N [1]	0.0484	3.013×10^7	-346	8243	0.4686
Lorenz [6]	0.0899	1.872×10^7	-114	2700	0.5198
Sprott B [1]	0.1380	5.632×10^3	-48	1015	0.6601

Discrepancies can be observed, as expected, when comparing the grades obtained in the present work (Table 5.1), which are derived from a fixed-point arithmetic implementation, with those reported in [4], which are based on floating-point arithmetic. Among the four evaluation parameters presented in Table 5.1, $d_{\mathcal{A}}$ is

the least affected by the transition from floating-point to fixed-point arithmetic, as the volume of $\mathcal{A}$ undergoes negligible variation in both implementations. On the other hand, the V_{Sub} parameter is significantly constrained by the fixed-point implementation since the size and shape of V_{IC} are altered due to the accumulation of quantization errors in both the ICs and the intermediate states of $\mathcal{A}$. Quantization errors also affect the trajectory of the intermediate states within $\mathcal{A}$, resulting in differences in the calculated DTR and MDT values.

Both floating-point and fixed-point arithmetic implementations are approximations of real chaotic maps found in nature. The digitization of natural chaotic systems inevitably introduces errors, which may cause the maps to deviate from chaotic behavior at some point during the simulation, a phenomenon known as dynamic degradation [165]. Such digital maps may eventually converge, diverge, or enter oscillatory modes, making their behavior predictable, an extremely undesirable characteristic in many applications of chaotic maps, particularly in cryptography. Although this behavior is inherent to the digital realization of chaotic maps (meaning it cannot be avoided with 100% certainty) the literature identifies three remedies [165] that can be applied to reduce the occurrence of dynamic degradation in digital chaotic systems: using higher finite precision, cascading multiple chaotic systems, and applying perturbation-based algorithms. In this work, we use higher finite precision both to combat dynamic degradation and to strengthen the encryption algorithm as evidenced in Section 5.4. The approach presented in this section also mitigates dynamic degradation by selecting a chaotic map that was extensively simulated prior to use in order to evaluate the four parameters $d_{\mathcal{A}}$, V_{Sub} , DTR, and MDT discussed above. The Maximum Dispersion Time (MDT) parameter was used to limit the digital simulation time, effectively helping to ensure that no dynamic degradation occurs during this early period of simulation ($0 < t < \text{MDT}$).

5.3 Chaos-Based Substitution Box (CB-SBox)

As stated in Section 5.2, the Sprott B chaotic system was selected for the construction of the CB-SBox proposed herein. This map was introduced by Sprott in 1994 [1] as part of a mathematical effort to identify simple algebraic three-

dimensional ordinary differential equations that exhibit chaotic behavior, resulting in the discovery of nineteen distinct systems. The Sprott B chaotic system is characterized by two critical points, $(1, 1, 0)$ and $(-1, -1, 0)$, and three Lyapunov exponents $\lambda = (0.210, 0, -1.210)$, where the largest exponent is positive as required for the emergence of chaos. Additionally, the system has a fractal dimension of 2.174, and its strange attractor $\mathcal{A}$ is illustrated later in this work (see Section 5.4.2). As shown in Equation (5.7), the Sprott B system features three integrators for $\dot{x}$, $\dot{y}$, and $\dot{z}$; two multipliers for yz and xy ; and two subtractors for $x - y$ and $1 - xy$. In Section 5.5, the CB-SBox is applied in a practical example, serving as the source of confusion in a Feistel network based on the block cipher proposed by Jakimoski in 2001 [24]:

$$\begin{cases} \dot{x} = yz \\ \dot{y} = x - y \\ \dot{z} = 1 - xy \end{cases} \quad (5.7)$$

The S-Boxes used in [24] are derived from Equation (5.8), where $g(\cdot)$ is obtained from a discrete chaotic map. The function f_j is defined in [24] through a procedure based on the N^{th} iteration of the logistic chaotic map. Essentially, the function f_j maps an 8-bit input to a pre-computed 8-bit output derived from the proposed procedure. The hardware implementation of f_j is straightforward: a ROM block with a depth of 256 positions and a word length of 8 bits. Jakimoski [24] employed eight such S-Boxes in his design, resulting in a 64-bit block cipher:

$$f_j = g(x_1 \oplus x_2 \oplus \dots \oplus x_j \oplus z_j) \quad (5.8)$$

For the present CB-SBox design, the function $f_j : M \rightarrow M$ defined by Equation (5.8), where $M = \{0, 1, \dots, 255\}$, is replaced by a digital realization of the Sprott B chaotic system from Equation (5.7). The complete CB-SBox schematic circuit view (the model is available online in [3]) is shown in Figure 5.2a, while Figure 5.2b presents the details inside the **Sprott_B** subsystem. Observe in Figure 5.2b the three integrators responsible for solving the chaotic system from Equation (5.7). The CB-SBox shown in Figure 5.2a has a single input, which is sliced into three ICs

$(x_0, y_0$ and $z_0)$, and correspondingly, a single output carrying the three final states $(x_f, y_f$ and $z_f)$. After properly setting the IC values inside V_{IC} (Figure 5.1), the circuit will run until an output uncorrelated from its input is obtained. The long running time (called LongRun in this work) is calculated by using the parameter DTR in Table 5.1 according to the *Discretization Criteria* (DCs) discussed in [2]. The DTR parameter is dependent on the minimal distance between successive ICs from V_{IC} (Figure 5.1).

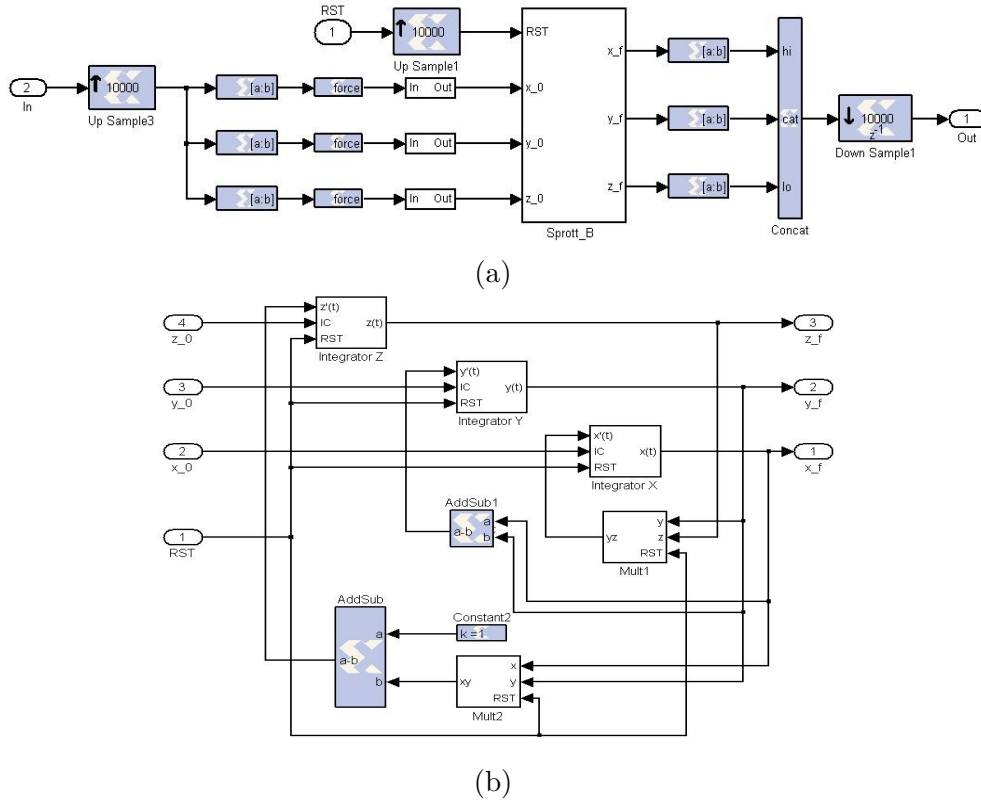


Figure 5.2: Schematic circuit view of the CB-SBox model and its Sprött B subsystem, available in [3]. (a) CB-SBox. (b) Sprött B [1] subsystem of Equation (5.7).

The parameters used to configure the circuit presented in Figure 5.2 are fully programmable and allow for the realization of the Sprött B-based CB-SBox in different lengths, i.e., the *Number of Bits* (NOB). Several precomputed parameters are stored in two configuration datasets, named *Parallelepiped Relations Measurements* (PRM) and *Slice*, which are available online in [3]. Each selected length (i.e., NOB) is associated with its own pair of datasets (PRM and Slice), built such that any CB-SBox input generates an initial condition (x_0, y_0, z_0) belonging to V_{IC} (see Figure 5.1). The values from the PRM and Slice datasets are used to configure the internal components of the programmable CB-SBox model (available in [3]), which

are then implemented in the circuit shown in Figure 5.2.

Each PRM dataset synthesizes, for a given NOB value, the dimensions of non-overlapping parallelepipeds within V_{IC} (see Figure 5.1) as exemplified in Table 5.2. Additionally, the PRM dataset lists, based on the selected dimensions and the applied DC, the bit lengths before and after the binary point for the limiting vertices of the (x, y, z) parallelepipeds, including their respective axial distances (Δ).

Table 5.2: The dimensions of three non-overlapping parallelepipeds belonging to the V_{IC} shown in Figure 5.1, available online in [3].

x_{min}	x_{max}	Δ	y_{min}	y_{max}	Δ	z_{min}	z_{max}	Δ
-12.125	-8.125	4	-4	4	8	-24	8	32
-8	8	16	-8	8	16	-8	8	16
8.125	12.125	4	-4	4	8	-24	8	32

The Slice dataset is specified by the NOB parameter and the values stored in the corresponding PRM dataset. The parameters contained in the Slice dataset are used to configure the force and slice blocks of the model shown in Figure 5.2b. The circuit depicted in Figure 5.2 operates under the control of a reset signal, whose period is defined by the internal parameter *Long Running Time* (LongRun). This reset signal initializes the CB-SBox to a new initial condition at the beginning of each LongRun cycle. It also controls the three integrators by triggering two dynamic registers within each one, both of which feature a configurable initial condition port. Additionally, the reset signal forces the two multipliers in Figure 5.2b to a null initial state at the start of each cycle. The integrators are further governed by an integration step size parameter (st), set to 0.01, and the multipliers operate with a latency parameter (Lat) of 5.

5.4 CB-SBox Performance Analysis

The main distinction between the block cipher presented in Section 5.5 and that introduced in [24] lies in the implementation of the S-Boxes. In the design proposed here, they are realized using the CB-SBox model described in Section 5.3 (see Figure 5.2). In contrast, the S-Boxes in [24] are implemented in this work, for

comparison purposes, as *Read Only Memory* (ROM) blocks populated through an offline procedure that precomputes the outputs of a chaotic system.

For fair comparison purposes, both designs (the CB-SBox from Section 5.3 and a ROM-based version implemented by the authors based on the method described in Jakimoski [24]) were synthesized in ASIC using VHDL. The synthesis tool employed was DC Synopsys, version Z-2007.03-SP4, for Linux, using the UMC CMOS 0.13 μm technology library. This setup ensures a more balanced comparison than FPGA-based implementations with VHDL code automatically generated by the system generator since specific architectural features in most FPGAs (such as embedded multipliers and memory blocks) can disproportionately impact resource usage, particularly the number of slices consumed.

5.4.1 Area and Power Analysis

A comparison is presented between area (μm^2) and power consumption (μW), both plotted along the y -axis, and circuit size (NOB), plotted along the x -axis. These comparisons are illustrated in Figures 5.3 and 5.4, respectively, for the ROM-based and CB-SBox implementations. The size is defined by the number of bits (NOB) of the circuit input, which equals the output size due to design symmetry.

As shown in Figures 5.3 and 5.4, both the area and power consumption of the ROM-based S-Boxes increase exponentially with NOB. For a ROM implementation with $\text{NOB} = 8$, meaning both input and output signals are 8 bits wide (corresponding to a memory depth of 256 positions), the area reaches $1.0861 \times 10^5 \mu\text{m}^2$ and the power consumption is $223.1284 \mu\text{W}$. When increasing the word length by one bit ($\text{NOB} = 9$), both area and power consumption nearly double, reaching $2.4612 \times 10^5 \mu\text{m}^2$ and $492.0213 \mu\text{W}$, respectively. Note that the ROM block was implemented up to $\text{NOB} = 13$; larger configurations could not be synthesized due to software and hardware limitations and had to be extrapolated.

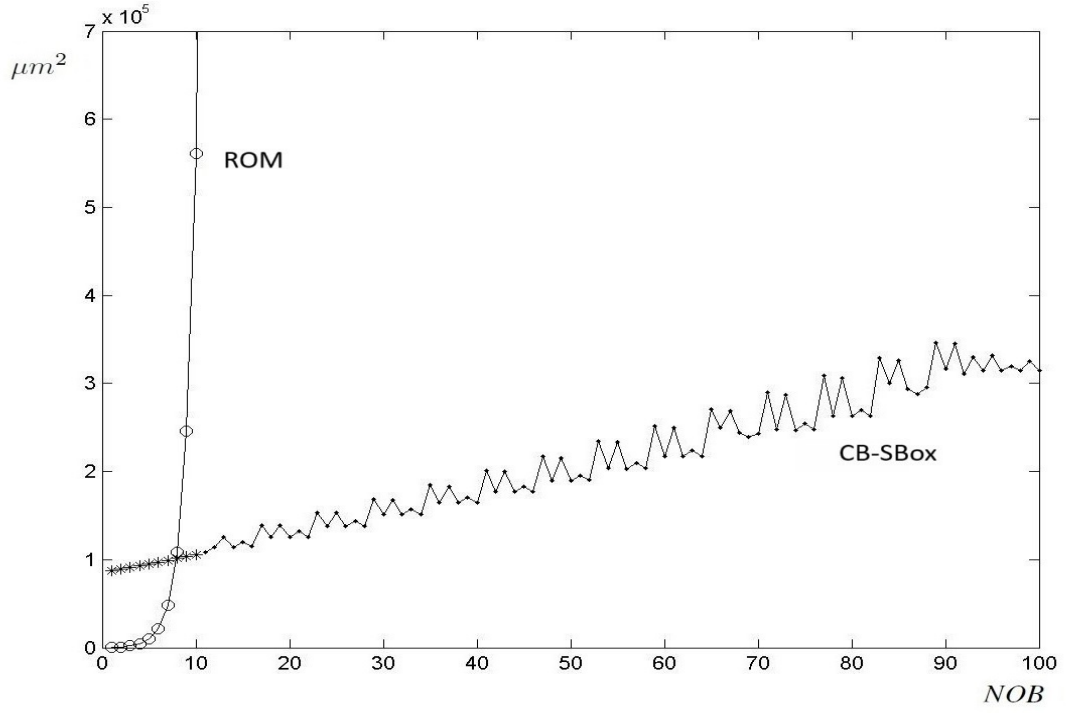


Figure 5.3: Area comparison between ROM-Based and CB-SBox implementations as a function of circuit input size (NOB).

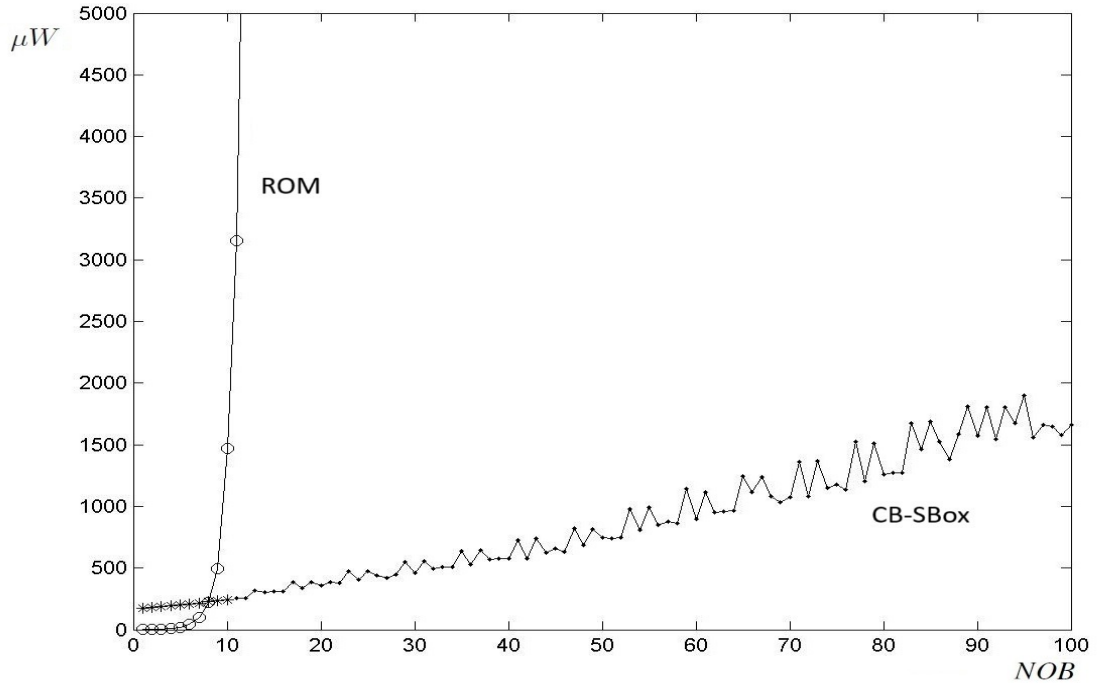


Figure 5.4: Power consumption comparison between ROM-Based and CB-SBox implementations as a function of circuit input size (NOB).

In the case of the proposed CB-SBox, as shown in Figures 5.3 and 5.4, there

is no strong exponential growth as observed in the ROM case. In fact, the CB-SBox consists of components (adders, subtractors, multiplexers, and registers), whose area and power consumption exhibit a nearly linear dependence on the circuit size (NOB). The only CB-SBox components with a non-linear dependence on NOB are the multipliers, but they do not significantly affect the overall area and power consumption of the circuit. Consequently, the area and power consumption of the CB-SBox increase almost linearly with NOB.

The area and power consumption of both ROM and CB-SBox designs are plotted together in Figures 5.3 and 5.4, respectively. In these figures, the strong exponential behavior of the ROM implementation is evident, in contrast to the nearly linear behavior of the CB-SBox implementation. It can also be observed that the equilibrium point occurs near $\text{NOB} = 8$, leading to the conclusion that for circuits requiring a word length greater than 8 bits, the CB-SBox design outperforms the ROM-based implementation in terms of area and power consumption.

5.4.2 Timing Analysis

Section 5.4.1 demonstrates that the area and power consumption of the CB-SBox implementation are superior to those of the ROM-based design for S-Boxes with $\text{NOB} > 8$. However, it is important to note that the latency of the CB-SBox implementation (defined by the LongRun parameter) is significantly higher than that of the ROM-based implementation. In chaos-based circuits, a substantially larger number of iterations is required to generate an output that is statistically decorrelated from its input (a condition that is often not thoroughly analyzed in existing implementations, as discussed in Chapter 3), whereas the ROM block delivers a precomputed value in a single clock cycle.

The LongRun parameter is determined by the defined Discretization Criterion (DC) [4]: the higher the DC, the larger the LongRun value required to decorrelate the CB-SBox input from its output. Based on the DC values stored in the PRM configuration dataset, Figure 5.5 shows the LongRun parameter (y-axis) as a function of the input size (NOB) of the CB-SBox circuit.

As shown in Figure 5.5, the relationship between the LongRun parameter and the NOB used in the CB-SBox realization exhibits an increasing pattern. The

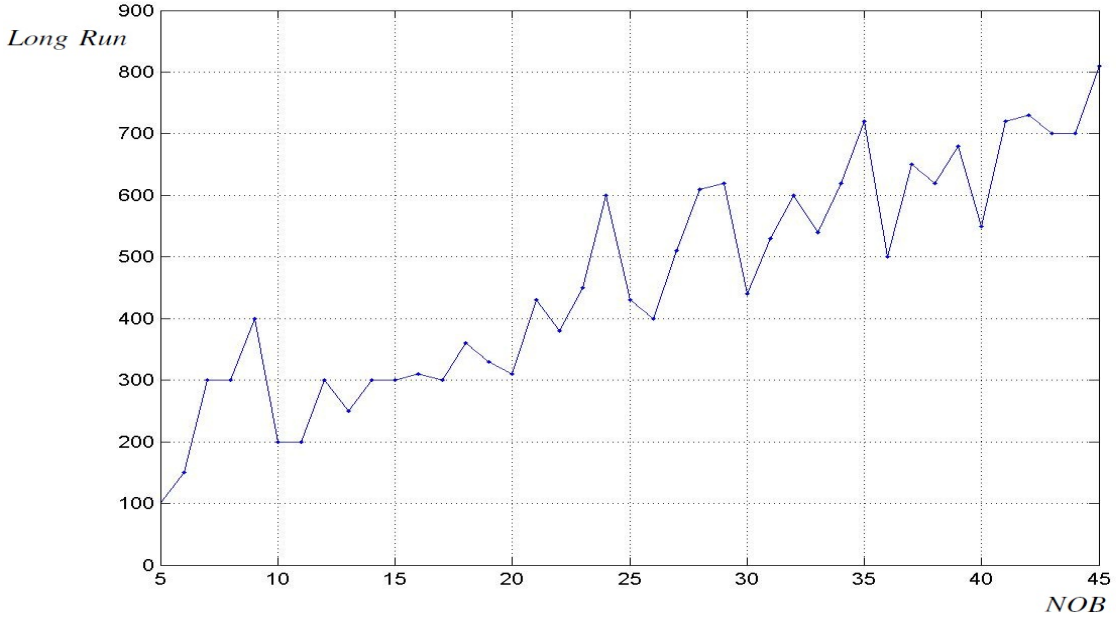


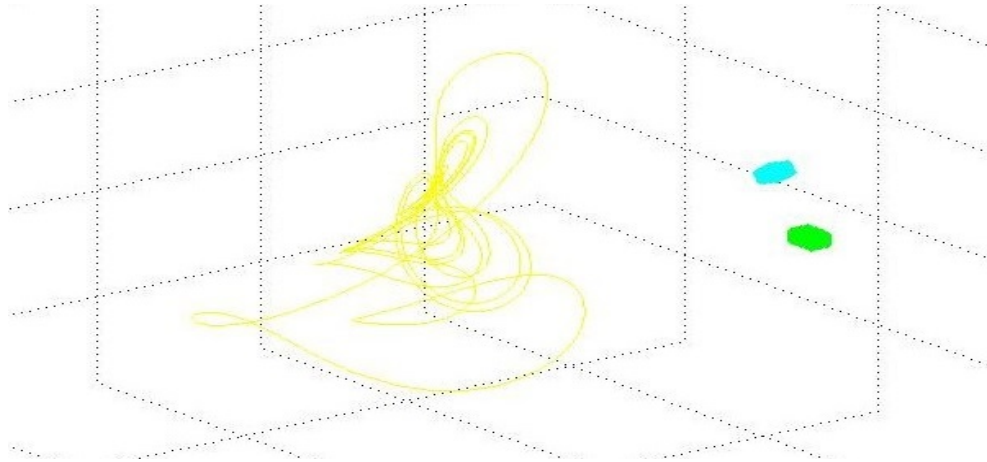
Figure 5.5: Time response of the CB-SBox: LongRun parameter required to decorrelate outputs from inputs, as a function of the circuit size measured in NOB.

data presented in Figure 5.5 were obtained through simulations of groups of 500 initial conditions (ICs). Each group of ICs was created using a specific Discretization Criterion ($4 \leq DC \leq 45$). The DC parameter is inversely proportional to the minimum distance between any pair of ICs within the group. The LongRun parameter represents the time required for each group of 500 ICs to fully disperse across the volume of the strange attractor $\mathcal{A}$ [4].

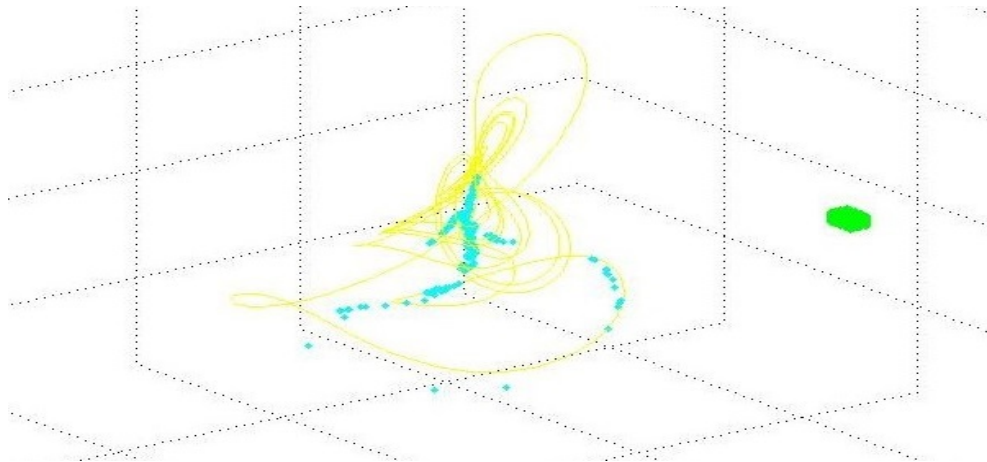
The location of each group of 500 ICs is a uniformly distributed random variable constrained within the volume of valid initial conditions (V_{IC}) [2]. Distinct groups, depending on their position within V_{IC} , exhibit different dispersion patterns. This behavior can be observed even in groups generated with the same DC, which results in the irregular behavior characterized by significant fluctuations as shown in Figure 5.5. This phenomenon is further analyzed below as detailed in Figure 5.8.

For illustration purposes, a three-dimensional cube of 729 ICs is plotted in Figure 5.6 in green. Its position is randomly assigned within $x \in [7.5085, 8.0085]$, $y \in [-3.3708, -2.8708]$, and $z \in [-2.1740, -1.6740]$. The Discretization Criterion (DC) is set to 4, resulting in a distance of 0.0625 between successive ICs, which facilitates the identification of the green cube in Figure 5.6. These 729 green ICs were simulated using Equation (5.7), and their corresponding final states are plotted

in blue. As expected, the final states tend toward the Sprott B strange attractor $\mathcal{A}$ (shown in yellow) and disperse across the attractor due to the butterfly effect. Figure 5.6 illustrates the three-dimensional dispersion pattern after 7 and 100 iteration steps. The project database, available online [3], includes 27 additional three-dimensional dispersion patterns up to 1900 iteration steps, provided in both JPG and FIG formats. To improve visualization, Figure 5.7 presents six two-dimensional graphs representing the temporal dispersion of ICs in blue, with the Discretization Criterion (DC) set to 5, over up to 500 iterations.



(a) Final states (blue) dispersed in $\mathcal{A}$ after 7 iteration steps



(b) Final states (blue) dispersed in $\mathcal{A}$ after 100 iteration steps

Figure 5.6: Visualization of a cube with 729 ICs (in green) and the three-dimensional dispersion of their corresponding final states (in blue) over the Sprott B attractor $\mathcal{A}$ (in yellow), available online in [3].

Despite extensive efforts (1300 groups of 500 ICs were simulated, each group constructed with DC equals to 30), no discernible pattern was identified linking the spatial locations of the IC groups within V_{IC} to the LongRun parameter. Figure 5.8

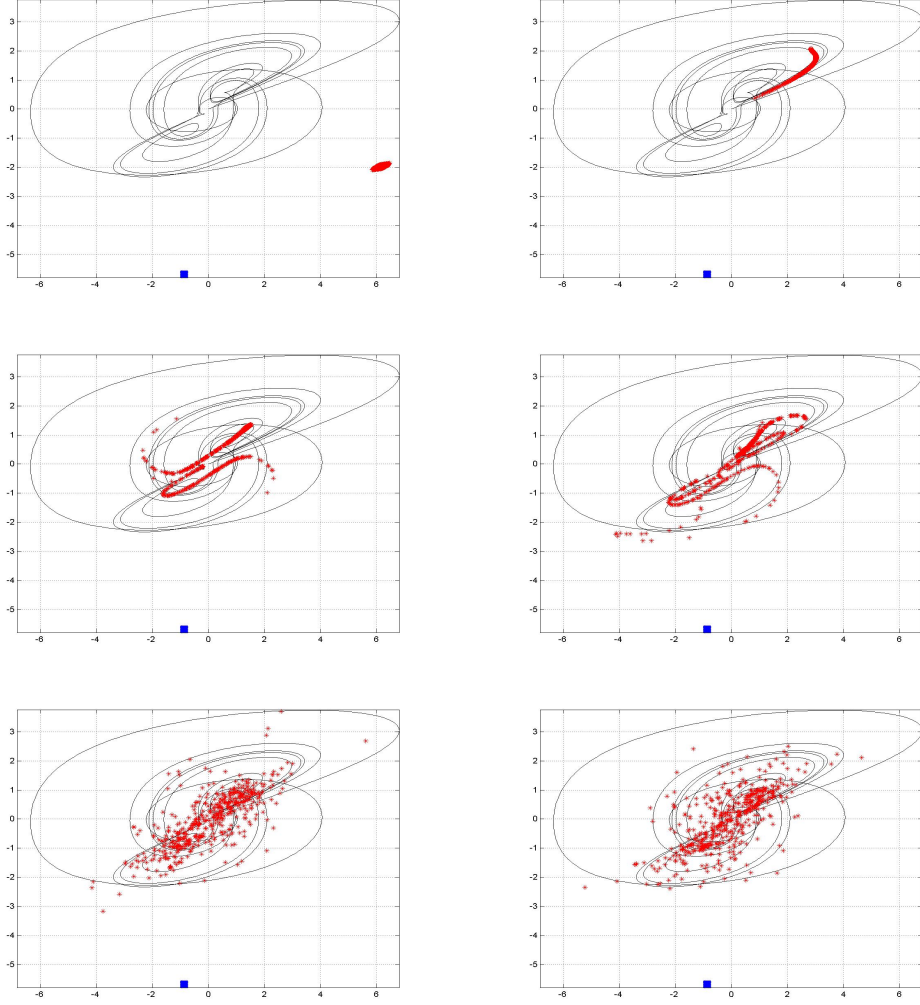


Figure 5.7: Visualization of a grid of ICs (blue) and the corresponding final state dispersion (red), generated by trajectories evolving on the Sprott B chaotic attractor $\mathcal{A}$ in a dimensionless state space. The results are presented as a 2D projection of the 3D phase space. The dataset is available online in [3].

illustrates the variation of the LongRun parameter with respect to the spatial distribution of the ICs groups within V_{IC} . This figure presents a representative subset of 79 IC groups. The center of each group is defined by its x- and y-axis coordinates shown in Figure 5.8, all of them at the same elevation of $z = -17.0625$. The LongRun parameter is encoded using the following seven-symbol scheme (not all symbols appear in the subset shown in Figure 5.8): a blue point $\bullet$ indicates that the required LongRun parameter lies within the interval $(420, 460]$; a green circle $\circ$ corresponds to $\text{LongRun} \in (460, 500]$; a red square $\blacksquare$ to $\text{LongRun} \in (500, 540]$; a cyan multiplication sign $\times$ to $\text{LongRun} \in (540, 580]$; a magenta addition sign $+$ to $\text{LongRun} \in (580, 620]$; a yellow lozenge $\diamond$ to $\text{LongRun} \in (620, 660]$; and a black

asterisk * to $\text{LongRun} \in (660, 700]$. The lack of a clear spatial correlation between group locations and the LongRun parameter suggests the influence of other contributing factors, potentially arising from the system's inherent chaotic dynamics, which warrant further investigation.

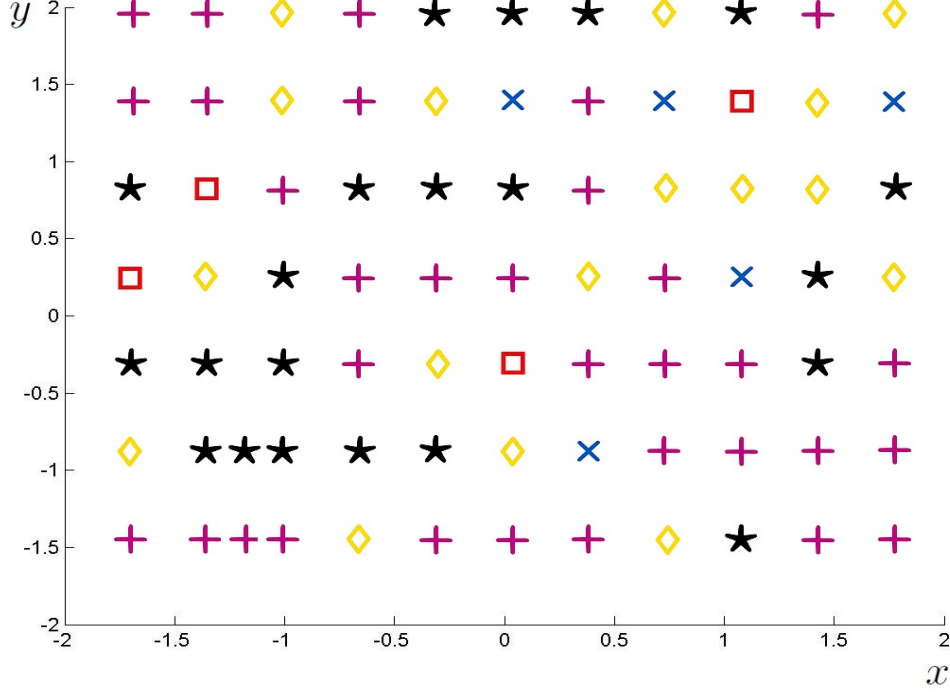


Figure 5.8: Spatial distribution of LongRun parameter (within the graph) for 79 groups of 500 ICs in the plane $z = -17.0625$, with $DC = 30$.

The timing analysis presented in this Section 5.4.2 is intrinsically linked to the circuit throughput. For a ROM-based S-Box, its contents are precomputed prior to runtime, and during operation, the output becomes available with minimal latency. In contrast, the CB-SBox proposed in this work generates outputs dynamically, which requires additional computation time during operation. This latency is governed by the LongRun parameter, which increases as the DC value decreases as previously discussed (Figure 5.5). Consequently, this behavior directly impacts the circuit throughput as will be further analyzed in Section 5.5, where the CB-SBox is applied to a practical implementation of a Feistel network based in [24].

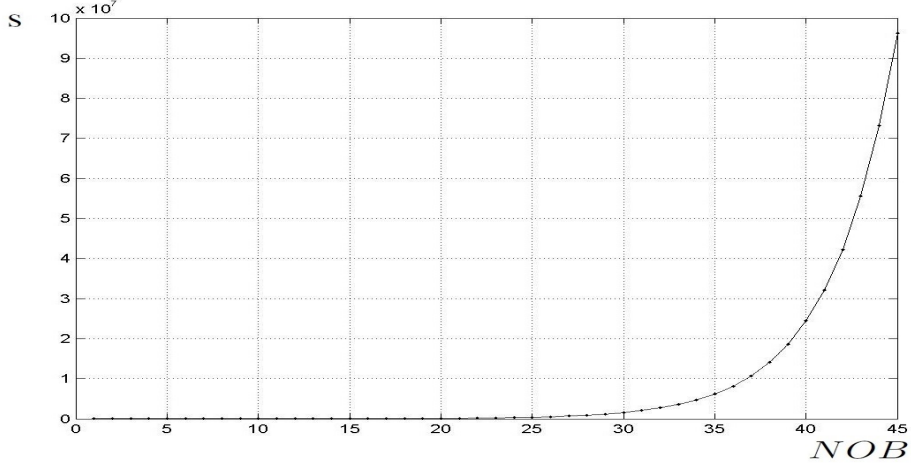
5.4.3 Security Analysis

Linear cryptanalysis [194] and differential cryptanalysis [195] are the two most prominent attacks applicable to cryptographic schemes [192]. These attacks rely on identifying structural weaknesses in the non-linear components responsible for confusion: the S-Boxes (the proposed CB-SBox in this work). The initial step in both techniques involves computing two quantitative parameters dependent on the properties of the S-Boxes: the Linear Probability Bias and the Differential Probability Bias.

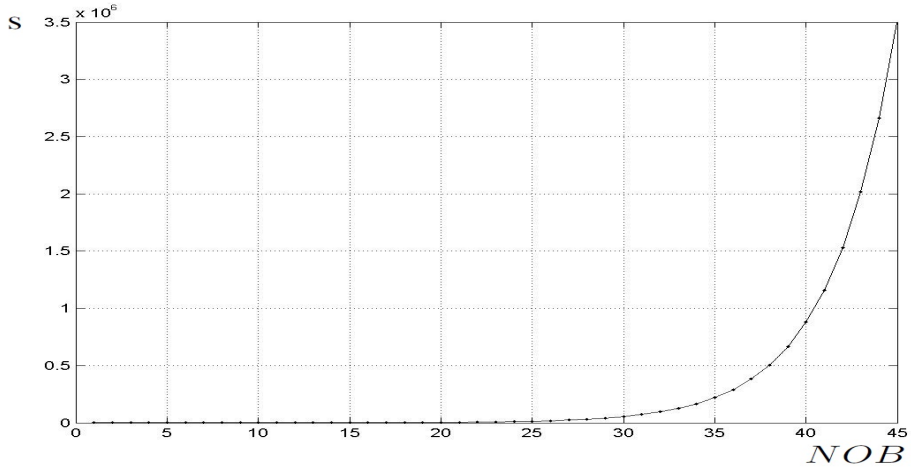
The effort required to compute the two parameters (Linear and Differential Probability Biases) increases exponentially with the NOB of the S-Box, as illustrated in Figure 5.9, which presents the computation time (in seconds) for each parameter calculation. The values for $\text{NOB} \leq 23$ were obtained through actual computations, while those for $\text{NOB} \geq 24$ were extrapolated based on the exponential behavior observed for the lower $\text{NOB} \leq 23$ values. The time required to compute the Linear and Differential Probability Biases represents the initial step in the cryptanalysis of a block cipher and does not directly indicate its resistance to these attacks. Rather, the cipher's vulnerability is determined by the magnitude of the resulting biases: lower bias values correspond to higher resistance to linear and differential cryptanalysis. Nevertheless, performing this computation is a necessary preliminary step in evaluating and strengthening cipher security. As shown in Figure 5.9a, computing the Linear Probability Bias for $\text{NOB} = 23$ required 10 days, and it is estimated that for $\text{NOB} = 43$, the process would take approximately 2 years. The proposed CB-SBox supports larger NOB values than conventional ROM-based S-Boxes, providing a strong initial barrier against cryptanalytic attacks.

5.4.4 Bijectivity Analysis

The proposed CB-SBox maps all possible inputs within V_{IC} (Figure 5.1) to their corresponding outputs by iterating the chaotic system defined in Equation (5.7) over a sufficiently long period (LongRun). This process enables the outputs to spread across the strange attractor $\mathcal{A}$ due to the butterfly effect, as illustrated in



(a) Computation time required to evaluate the Linear Probability Bias.



(b) Computation time required to evaluate the Differential Probability Bias.

Figure 5.9: Security analysis based on the computation time (seconds) in y-axis required to evaluate the Linear and Differential Probability Biases of S-Boxes as a function of their size (NOB) in x-axis, available online in [3].

Figure 5.6. As a result of the inherent nature of chaotic systems (characterized by sensitive dependence on ICs and the fractal structure of strange attractors) iterating Equation (5.7) for an extended duration causes the outputs to become not only widely dispersed across the attractor but also potentially mapped to locations already assigned to other outputs, leading to an inherently non-bijective behavior.

CB-SBox with different NOBs were simulated, and the results are summarized in Table 5.3. Their deterministic outputs were stored in matrices referred to as SBOX Chaotic, each of length 2^{NOB} as specified in Table 5.3. Additional matrices of identical dimensions, named SBOX Chaotic Counter, were employed to record the number of times each output value occurred during the simulations. For a matrix to

be considered bijective, each output must appear exactly once, which corresponds to a bijectivity index of 100%, meaning that the number of ones (1s) in the SBOX Bijective Counter matrix is 100%.

Due to their chaotic nature, the proposed CB-SBox is inherently non-bijective, exhibiting a mean bijectivity index of 63.57% across the simulated cases presented in Table 5.3. This indicates that only this proportion of possible outputs was mapped by the CB-SBox during the simulations, while the remaining 36.43% of outputs were never mapped, corresponding to the proportion of zeros (0s) in the *SBOX Chaotic Counter*. The complete statistical dataset referenced in this analysis is available online in [3].

Table 5.3: Statistical analysis of the bijectivity of CB-SBoxes, where NOB denotes the number of bits, followed by the corresponding table length that equals 2^{NOB} and the calculated bijectivity index (data available online in [3]).

NOB	Length	Bijectivity
11	2048	63.48%
12	4096	63.16%
13	8192	63.09%
14	16,384	62.91%
15	32,768	63.43%

The lack of bijectivity is a factor that must be considered from a holistic perspective as discussed in more detail in Section 5.4.5. S-Boxes are integral components of various cryptographic schemes, primarily introducing non-linearity and confusion to enhance security. Traditionally, S-Boxes are bijective, which is crucial for invertibility in some cryptographic processes. However, certain cryptographic schemes, such as hash functions, stream ciphers, specific cryptographic protocols, and Feistel networks, can employ non-bijective S-Boxes, where the lack of bijectivity does not compromise security or functionality as demonstrated in other scientific works [36, 39].

5.4.5 Joint Analysis

As discussed in Section 5.4.1, when dealing with large S-Boxes ($\text{NOB} \gg 8$), it is more advantageous to implement a CB-SBox rather than using a ROM-based approach due to the exponential growth of the latter, resulting in significantly smaller circuits with lower power consumption when using the CB-SBox solution.

However, as pointed out in Section 5.4.2, this approach results in slow response times: due to the Butterfly Effect [193], chaotic behavior takes a long time to fully develop as shown in Figures 5.5 and 5.6.

The analysis presented in Section 5.4.3 shows that, despite its slow response time, the CB-SBox is a valuable approach for enhancing the security of block ciphers: the CB-SBox enables the implementation of large S-Boxes, which enhances the cipher's resistance to linear and differential cryptanalysis as shown in Figure 5.9.

The bijectivity of the proposed CB-SBox is analyzed in Section 5.4.4. The CB-SBox exhibits a mean bijectivity index of 63.57%, indicating non-bijective behavior resulting from the chaotic nature of the Sprott B [1] map used within. Several scientific works have addressed this issue by the offline substitution of repeated S-Box outputs. However, this approach was not adopted in the present research, as it would undermine the primary advantage sought in this work: the emulation of a large S-Box computed OtF.

It is worth noting that the CB-SBox design not only facilitates the implementation of large S-Boxes ($\text{NOB} > 35$) but also achieves this with smaller circuits (lower area) and reduced power consumption, compared to a equivalent ROM-based implementation. A realizable 30-bit CB-SBox, with a security level equivalent to that of a 30-bit non-realizable (within the scope of this work) ROM implementation, both requiring 17 days for the Linear Probability Bias calculation, consumes only 0.0004% of the area and power needed by the 30-bit ROM.

Therefore, the joint analysis presented here in Section 5.4.5 demonstrates that the CB-SBox offers an effective solution when a high level of security is required. The latency issue addressed in Section 5.4.2 can be mitigated by the compact area and low-power-consumption characteristics of the CB-SBox, with a parallel circuit implementation serving as an alternative to attenuate the high-latency problem

discussed in Section 5.4.2. Further details regarding this are provided in Section 5.5, which focuses on the Feistel network implementation using the proposed CB-SBox.

5.5 CB-SBox in a Feistel Network

The CB-SBox developed in this work was employed in the construction of a Feistel network based on the architecture proposed by Jakimoski [24]. In the present study, the precomputed ROM-based S-Boxes utilized in [24] were substituted by the proposed CB-SBox, which is detailed in Section 5.3 and analyzed in Section 5.4.

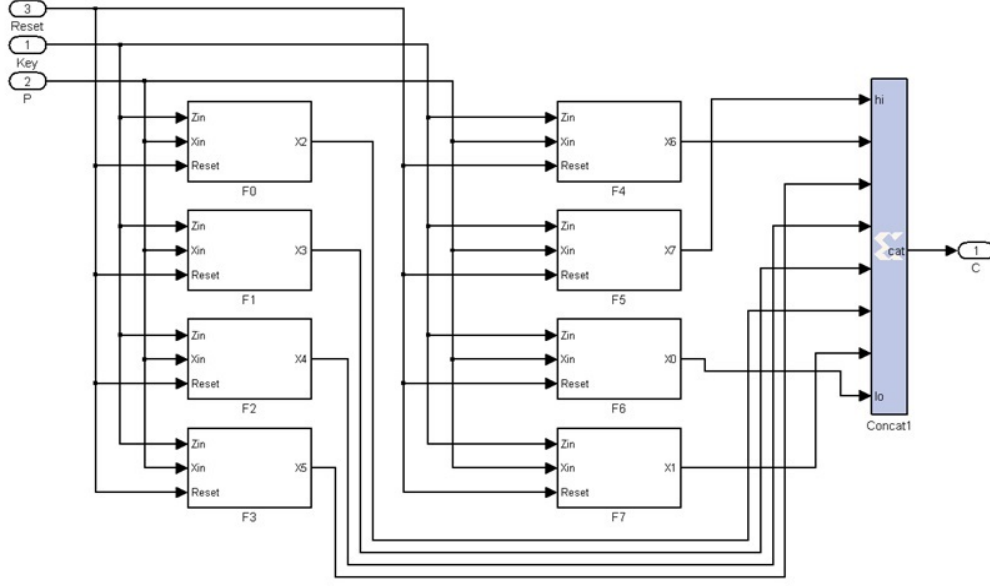
The schematic diagram of the designed block cipher is shown in Figure 5.10, which implements Equation (5.9), obtained from Jakimoski’s work [24]. Figure 5.10a illustrates the complete block cipher with its three inputs: the plaintext B_0 divided into x_k words, where $k = 1, 2, \dots, 8$; the round-related subkeys z_i , where $i = 1, 2, \dots, r$; and the *reset* signal. Figure 5.10a also shows its output, which is the ciphertext B_r , obtained after r rounds:

$$x_{i,k+1} = x_{i-1,k} \oplus f_{k-1}[x_{i-1,1}, \dots, x_{i-1,k-1}, z_{i-1,k-1}] \quad (5.9)$$

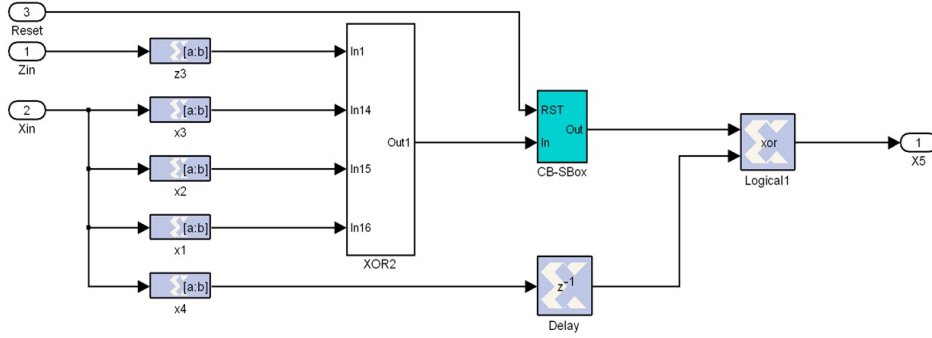
Figure 5.10b illustrates the internal details of subsystem f_3 in Figure 5.10a, where the CB-SBox subsystem is highlighted in blue (its schematic diagram is presented in Figure 5.2). All subsystems f_0 to f_7 in Figure 5.10a exhibit a similar structure to the one shown in Figure 5.10b, each containing one CB-SBox but with an XOR port having different inputs as described by Equation (5.9).

As discussed in Section 5.3, the CB-SBox is a programmable circuit whose word length ($11 < \text{NOB} < 41$) can be configured through PRM and Slice datasets available online in [3]. Consequently, since the block cipher illustrated in Figure 5.10 comprises eight CB-SBoxes, the total word length processed by the cipher can be programmed to range from 88 to 328 bits. In the example shown in Figure 5.10, the cipher is implemented with a total word length of 136 bits.

The block cipher is implemented recursively: only a single round of the cipher is physically realized, and the intermediate encrypted words B_i are fed back to the input $r - 1$ times to complete the required r rounds of encryption, where $i = 1, 2, 3, \dots, r - 1$.



(a) Feistel network using the proposed CB-SBox.



(b) Internal details of subsystem f_3 .

Figure 5.10: Schematic diagram of the encryption block cipher, where the CB-SBox, embedded within each f_k subsystem and previously detailed in Figure 5.2, is highlighted in blue.

The decryption architecture is derived from Equation (5.10), as presented in [24], by applying the inverse transformations defined in Equation (5.9): the round subkeys z_i are applied in reverse order, and the same number of rounds r are performed on the ciphertext block B_r to recover the original plaintext block B_0 . The decryption operation involves series connections between the f_k blocks, requiring eight times as many clock cycles to complete its tasks compared to encryption, due to the feedback arrangement shown in Figure 5.11:

$$x_{i-1,k} = x_{i,k+1} \oplus f_{k-1}[x_{i-1,1}, \dots, x_{i-1,k-1}, z_{i-1,k-1}] \quad (5.10)$$

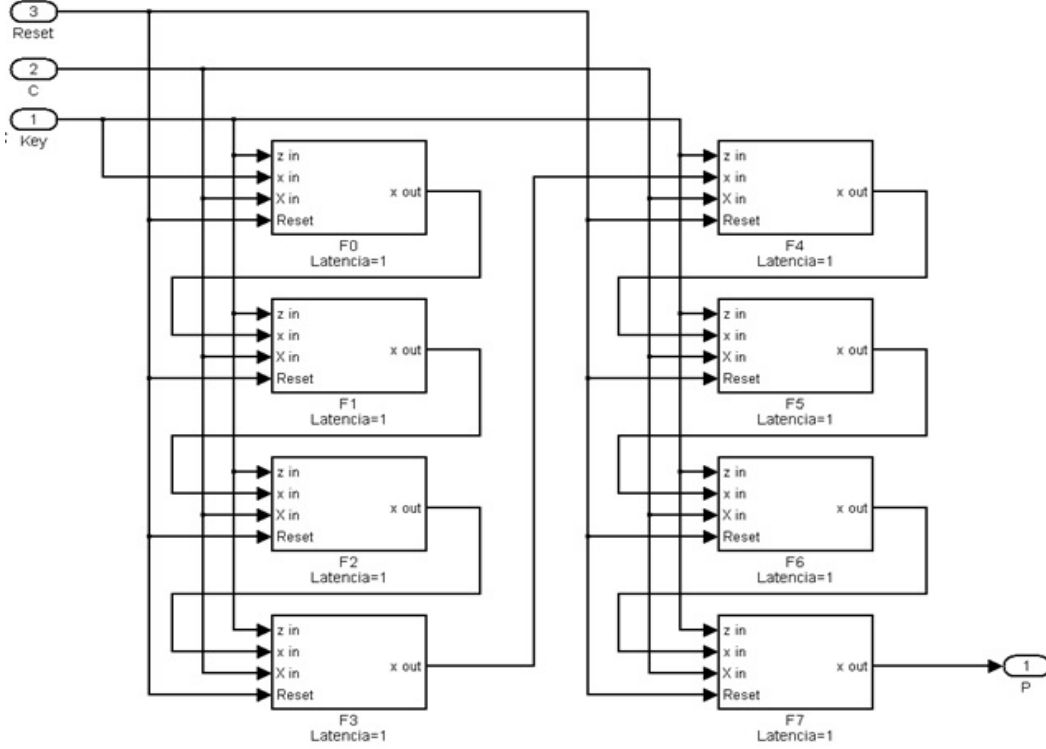
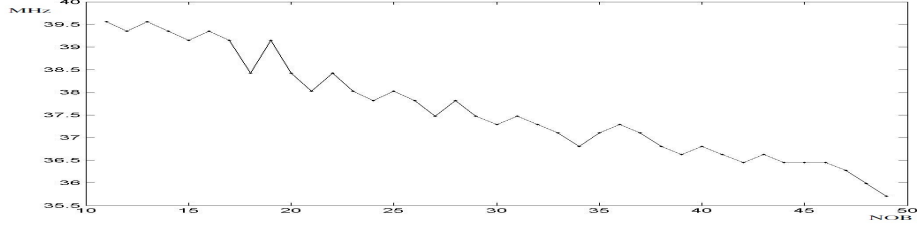


Figure 5.11: Schematic representation of the decryption block cipher.

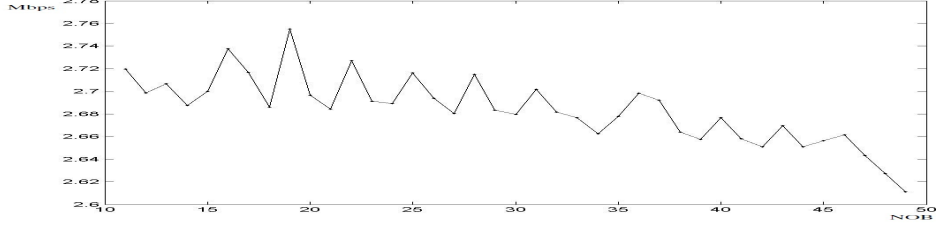
The block cipher implementation results in a multi-rate circuit as a result of the presence of up and down samplers in the architecture shown in Figure 5.2, which are integrated within the CB-SBox subsystem depicted in Figure 5.10b. These samplers are necessary to compensate for the latency introduced by the multipliers, which equals five clock cycles, and the integration step size, set to 0.01. These parameters are used in the implementation of the Sprott B differential chaotic system defined in Equation (5.7). The block cipher operation is controlled by a reset signal, which synchronizes the loading of ICs with the cycle initialization, governed by the LongRun parameter.

The performance analysis of the FPGA-implemented block cipher is presented in Figure 5.12. This figure includes four graphs, each plotted as a function of the NOB (x-axis): the size of the proposed programmable CB-SBox. Figure 5.12a shows the maximum operating frequency of the circuit, measured in MHz (y-axis). As the size of the CB-SBox increases, the maximum frequency decreases as expected. Based on Figure 5.12a, the interval $11 < \text{NOB} < 20$ was selected as the target design range.

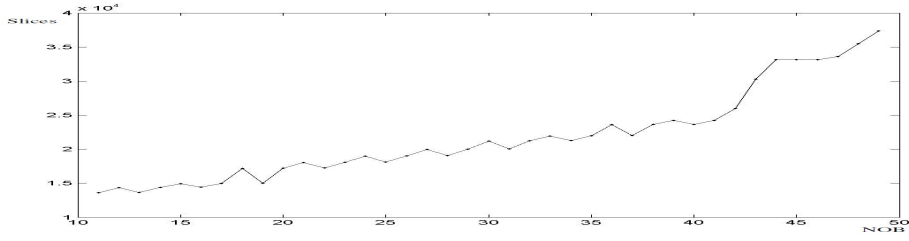
Figure 5.12b illustrates the data rate, measured in Mbps (y-axis), computed



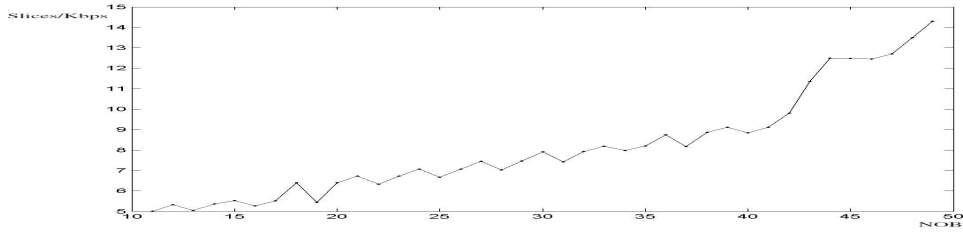
(a) Maximum Frequency (MHz)



(b) Data Rate (Mbps)



(c) FPGA Resource Utilization (Slices)



(d) Circuit Cost (Slices/Kbps)

Figure 5.12: FPGA performance of the block cipher.

as the product of the maximum circuit frequency and the size of the encrypted word, while accounting for the compensation required by the LongRun parameter. As discussed in Section 5.4.2, the timing analysis of the CB-SBox is intrinsically linked to the circuit throughput. In ROM-based S-Box architectures, the output is available with minimal latency. In contrast, the CB-SBox proposed in this work incurs additional computational delay during execution. As a result, this behavior directly impacts the overall throughput of the cipher. Figure 5.12b reveals a peak data rate of 2.755 Mbps at $\text{NOB} = 19$, which is significantly lower than the typical 10 Mbps achieved by ROM-based implementations.

The remaining two graphs present the hardware resource utilization, measured in FPGA slices as shown in Figure 5.12c, and the circuit cost, measured in slices per Kbps as presented in Figure 5.12d. Both graphs exhibit a local minimum at $\text{NOB} = 19$, justifying the selection of this value as the optimal operating point for the proposed CB-SBox architecture.

The selected operating point ($\text{NOB} = 19$) lies within the region where the CB-SBox demonstrates superior performance in terms of area efficiency and power consumption compared to ROM-based S-Box implementations, as illustrated in Figures 5.3 and 5.4. These results indicate that a 19-bit CB-SBox implementation requires only 0.0238% of the area and 0.0241% of the power consumed by its securely equivalent yet physically unrealizable ROM-based counterpart. It is important to note that the proposed CB-SBox represents the only modification to the block cipher architecture described in [24]. Furthermore, $\text{NOB} = 13$ corresponds to the largest feasible ROM-based implementation attainable with the hardware and software resources available in the laboratory.

As discussed in Section 5.4.5, the main advantage of applying the CB-SBox to the Jakimoski-based cipher [24] is the ability to implement large S-Boxes ($\text{NOB} \gg 8$), thereby achieving high levels of resistance against linear and differential cryptanalysis. The block cipher designed in this work, which employs a 19-bit CB-SBox, requires approximately 20 hours to compute the Linear Probability Bias and 38 minutes to compute the Differential Probability Bias as shown in Figure 5.9. Such a 19-bit implementation would not be feasible using a ROM-based approach. It is also important to emphasize that this analysis represents only the initial step in the process of attacking a cipher through linear and differential cryptanalysis.

The described 152-bit recursive block cipher, which employs the proposed CB-SBox and is configured with four rounds, was applied to the grayscale ‘Lena’ image, as illustrated in Figure 5.13a. The image was converted into a 512×512 matrix, with each pixel represented by 8 bits. To match the cipher’s 152-bit block size, bit padding with 18 one bits was applied. The padded data were then encrypted, and the resulting cipher image is presented in Figure 5.13b. After decryption, the 18 padding bits were removed from the final block, restoring the original 512×512 matrix. The decrypted image is shown in Figure 5.13c. The FPGA-based implemen-

tation of the block cipher required 6.09 s for encryption and 51.76 s for decryption.

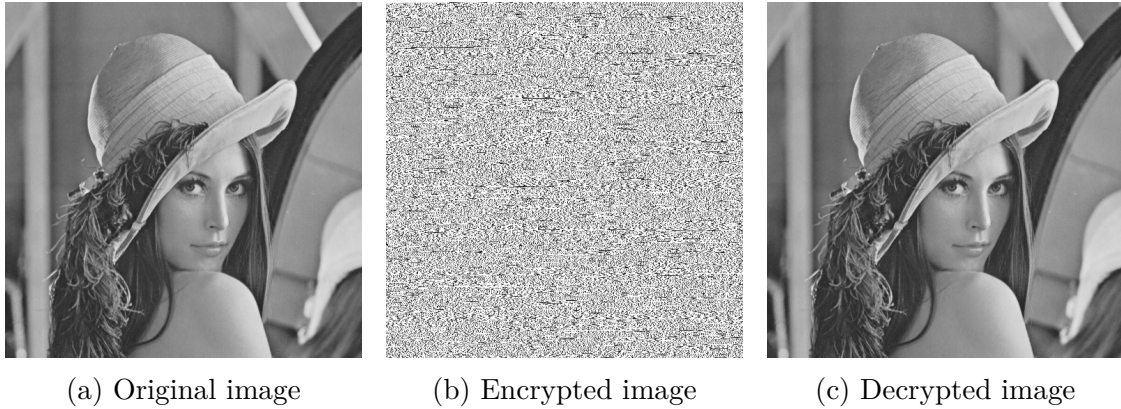


Figure 5.13: Results of applying the 152-bit recursive block cipher to the ‘Lena’ image.

Besides image encryption, the 152-bit block cipher described in this section, employing the proposed CB-SBox, was also applied to text encryption. A initial abstract version of this chapter, shown in the upper part of Figure 5.14, was converted into a 1691-bit character string, padded with 14 one bits, and used as the plaintext. The corresponding ciphertext is shown in the lower part of Figure 5.14. Since the plaintext is based on a LaTeX text fragment, it consists solely of basic ASCII characters, corresponding to codes ranging from 0 to 127, even after one-bit padding, and is represented using 8-bit encoding, which accommodates values from 0 to 255. In contrast, the ciphertext utilizes the full 8-bit ASCII range and, therefore, includes special characters with codes between 128 and 255. As some special characters cannot be properly represented graphically, a hexadecimal representation is employed as illustrated in the lower part of Figure 5.14. This behavior is further observed in Figure 5.15, which presents the plaintext histogram (Figure 5.15a) ranging from 0 to 127, the flattened ciphertext histogram (Figure 5.15b) ranging from 0 to 255, and the deciphered text histogram (Figure 5.15c) ranging from 0 to 127 but exhibiting a small peak in the left due to the one-bit padding, which does not appear in the plaintext histogram (Figure 5.15a) as expected.

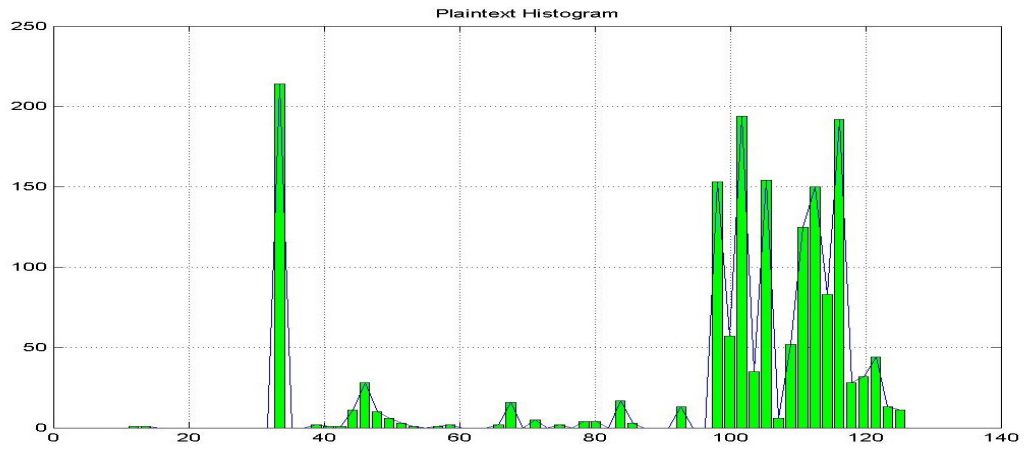
Plaintext:

\abstract{In recent years, many chaos-based encryption algorithms have been proposed. Many of these are based on established designs and populate their S-Boxes with values derived from chaotic maps, following conventional implementation strategies to enable comparison with their original non-chaotic counterparts. In contrast, this work proposes a novel approach: a \mbox{Chaos-Based} Substitution Box (CB-SBox) implementation, in which conventional \mbox{ROM-based} S-Boxes are replaced by a digital circuit that directly executes a selected chaotic map. This method enables the construction of \mbox{S-Boxes} with long word lengths through an FPGA-based programmable circuit that allows for variable S-Box lengths, facilitating the analysis of S-Boxes of varying sizes, and ultimately enhancing security, particularly for larger S-Boxes, as demonstrated by increased resistance to linear and differential cryptanalysis. Furthermore, the proposed CB-SBox achieves reductions in both area and power consumption compared to size-comparable \mbox{ROM-based} \mbox{S-Boxes}. A 19-bit \mbox{chaos-based} \mbox{S-Box} consumes just \mbox{0.0238\%} of the area and \mbox{0.0241\%} of the power required by an equivalent \mbox{ROM-implemented} S-Box while providing the same level of security. The inherent unpredictability of non-linear chaotic behavior causes the proposed chaos-based S-Boxes to exhibit non-bijective characteristics, making them well suited for application in non-invertible cryptographic primitives, such as hash functions and Feistel networks. The proposed CB-SBox was implemented in a Feistel network as described in the literature, and the results are provided.}

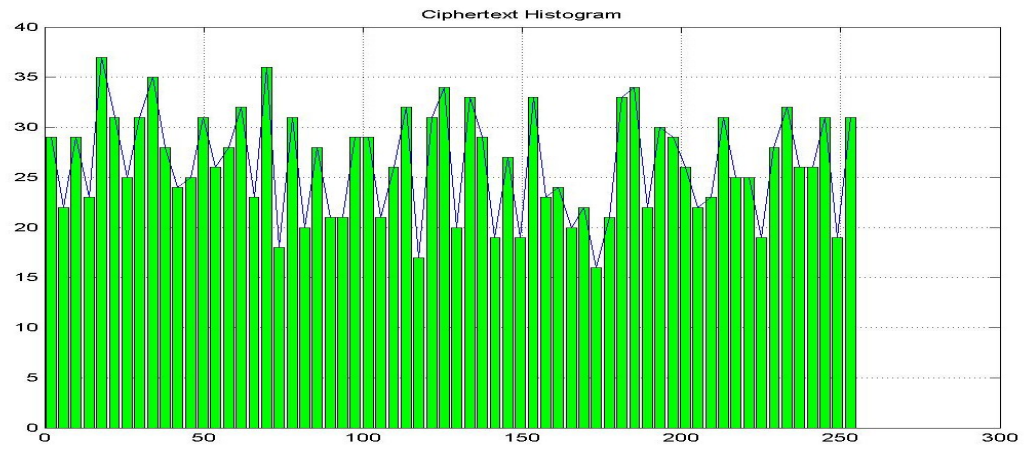
Ciphertext:

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

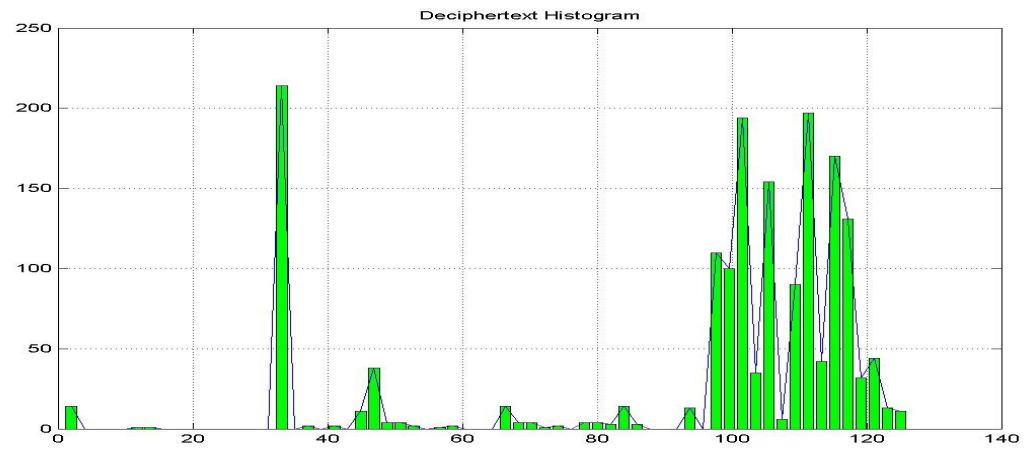
Figure 5.14: Original and encrypted versions of the LaTeX text, encrypted using the 152-bit recursive block cipher based on the CB-SBox.



(a) Plaintext histogram



(b) Ciphertext histogram



(c) Deciphered text histogram

Figure 5.15: Histograms after applying the 152-bit encryption process, which employs the proposed CB-SBox, to the abstract of this paper, written in LaTeX. The corresponding dataset is available online [3].

5.6 Chapter Conclusions - CB-SBox

This research presents a novel approach for the design of Feistel-type block ciphers. It is based on the fixed-point realization of a non-linear differential equation exhibiting chaotic behavior. This realization, referred to as the Chaos-Based Substitution Box (CB-SBox), enables the implementation of large and secure S-Boxes. These entities provide significant advantages in terms of area efficiency and power consumption when compared to conventional ROM-based s-boxes: a 19-bit CB-SBox requires only 0.0238% of the area and 0.0241% of the power consumed by an equivalent but physically infeasible ROM-based implementation. Furthermore, they achieve a high level of security, as measured by the time required to compute the first step of linear and differential cryptanalysis, which is practically infeasible for their ROM-based counterparts

As a consequence of the butterfly effect, this approach exhibits the disadvantage of a long iteration time, governed by the LongRun parameter, which is required to decorrelate the CB-SBox input signals (the chaotic system's ICs) from its output (the chaotic system's final states). This drawback is an intrinsic characteristic of applying chaos theory: the butterfly effect inherently requires time to manifest. This limitation is often neglected or not precisely evaluated in chaos-based cryptography and is naturally disregarded when a non-OtF technique is employed, as this temporal overhead disappears in such cases.

The CB-SBox was employed as the source of confusion in a block cipher based on the architecture proposed by Jakimoski [24]. This cipher was implemented using a programmable circuit, where the CB-SBox can be realized with different sizes, according to the parameters stored in the PRM and Slice datasets (available online in [3]). This enables a block cipher with a programmable key size. We analyzed the performance of the block cipher as a function of the size (NOB) of its CB-SBox, deciding to operate at $\text{NOB} = 19$ as a solution to globally maximize the circuit data rate while keeping the circuit size low and achieving high levels of security.

To conclude this Chapter, six open research areas have been identified and are discussed below. When a given group of ICs (ICs), belonging to the volume of valid initial conditions (V_{IC}), is stimulated by a chaotic system, it disperses into

the volume of the strange attractor $\mathcal{A}$ due to the butterfly effect. The temporal evolution pattern of the intermediate states may lead to the misleading conclusion that, depending on the relative position of this group of ICs, more time would be required for it to fully disperse throughout the attractor. The results presented in Figure 5.8 suggest an inconclusive relationship, making the correlation between the position of a group of ICs *versus* dispersion time a promising topic for future investigation.

Another potential research direction involves the implementation of a programmable Chaos-Based Substitution Box, in which not only the S-Box length (NOB) can be configured (as demonstrated in the present CB-SBox) but also the chaotic system itself can be dynamically altered. This capability would enhance the adaptability and security level of the target encryption primitive.

In this study, the Sprott B chaotic system [1] was selected among six other candidates, based on the criteria provided in [4]. The computation of chaotic properties such as V_{IC} is highly time-consuming but is worthwhile since it not only allows for a better use of the chaos map in the encryption process but also directly addresses quantization errors and dynamical degradation. A valuable extension of the present work would be to replicate the methodology of [4] using other chaotic systems, including hyperchaotic systems, higher-dimensional systems, systems exhibiting multiple attractors, and those with greater ergodicity as found in the literature [50, 52, 56, 121, 123]. It is expected that a chaotic system with improved ergodicity could reduce the LongRun parameter, thus increasing encryption throughput, and can also flatten the histogram plot of Figure 5.15b, combating a potential weakness of the proposed C-SBox: its capability to better spread the final states over all state space.

Non-bijective S-Boxes, like the proposed CB-SBox, are suitable only for specific types of cryptographic primitives, such as the Feistel network implemented in this work. An additional future direction includes the usage of the CB-SBox concepts in the design and evaluation of hash functions (non-invertible primitives) along with their implementation in ASIC.

This research also evaluated the CB-SBox's resistance to linear and differential cryptanalysis, demonstrating that larger S-Box sizes contribute positively to

security. Future work could include exploring alternative attack vectors reported in the literature, as well as proposing novel attack strategies specifically tailored to the developed CB-SBox solution.

In the present work, the primary focus is the comparison between the proposed chaos-based S-Box (CB-SBox) and a ROM-based implementation. Other approaches to implementing S-Boxes, such as logic gate designs, are also available. Although such implementations typically focus on small S-Boxes, there is no fundamental impediment to implementing larger ones and comparing them with the CB-SBox, which is suggested as future work.

Chapter 6

Conclusions

Reflecting on Achievements and Future Directions in Chaos-Based Cryptography

6.1 Timeline

According to the schedule presented in Table 6.1, the first semester of the PhD program (Semester 24.1) was primarily dedicated to completing the coursework required by the PPGEE at UFAM. During this period, all 12 required credits were successfully completed, including one mandatory course (PGENE600) and two elective courses (PGENE537 and PGENE549), selected by the PhD candidate Élvio Dutra and approved by the supervisor, Prof. Carlos Cruz.

Concurrently, the Supervised Study I course (PGENE614) was undertaken, during which the paper entitled “A Frugal Integrated Circuit Packaging for Non-Planar Surface-Conformant Electronics Applications” [196] was prepared and submitted to the SBCCI 2024 conference by the *SENAI Institute of Innovation in Microelectronics - Instituto SENAI de Inovação em Microeletrônica* (ISI-ME), with the PhD candidate participating as a coauthor. The ISI-ME is an *Research and Development* (R&D) institute of the *Brazilian National Industrial Training Service - Serviço Nacional de Aprendizagem Industrial* (SENAI). This publication extends previous work entitled “Reliability Aspects and Study of Copper Seed Deposition on Polyimide via Sputtering” [197], which was submitted to SBCCI 2023 by the same ISI-ME research team. Additionally, eleven papers [198–208] were reviewed during

this first semester as part of the Supervised Study I (PGENE614) activities.

The second semester of the PhD program (Semester 24.2) was primarily dedicated to advancing the research activities associated with the doctoral thesis. As part of the Supervised Study II course (PGENE615), the “Theoretical Framework” (Chapter 2) of this thesis was preliminarily developed, covering the following topics: chaos and cryptography, encryption foundations, chaos theory, scientific foundations, properties of chaotic systems, and their applications in cryptography. Also in Semester 24.2, a paper entitled “Current Mirror Improved Potentiostat (CMIPot) for a Three-Electrode Electrochemical Cell” [209] was submitted to the journal *Sensors* (MDPI), with the PhD candidate acting as a coauthor.

The third semester of the PhD program (Semester 25.1) was primarily dedicated to research activities as part of the Supervised Study III course (PGENE616). During this semester, two papers were submitted: “A Novel Wi-Fi Independent Wireless Network Architecture for Industry 4.0 and IIoT Applications” [210], submitted to the 2025 International Symposium on IoT (SIoT), with the PhD candidate participating as a coauthor; and “Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives” [180], submitted to the journal *Electronics* (MDPI), a Qualis A4 journal according to the CAPES Sucupira platform, with the PhD candidate as the first author. The journal has an impact factor of 2.6 and a CiteScore of 6.1, according to MDPI. This second paper was published on 28 May 2025 and received its first citation on 21 Oct 2025 [211], subsequently cited in [212–215]. This publication fulfills the minimum publication requirements outlined in the document “Guia Rápido – Recomendação,” officially published on 2 December 2024 by the PPGEE coordination at UFAM.

To conclude the third semester, the PhD candidate Élvio Dutra underwent the Qualification Examination on 30 June 2025 at 09:00 AM (AMT), conducted at the CETELI auditorium and remotely via Google Meet. The examination committee comprised Prof. Dr. Carlos Augusto de Moraes Cruz (UFAM, CETELI), Prof. Dr. Paulo Fernandes da Silva Júnior (UEMA), and Prof. Dr. Eduardo Luzeiro Feitosa (UFAM, iComp). The PhD candidate was approved and authorized to proceed with the activities outlined in Table 6.1.

The fourth semester of the PhD program (Semester 25.2) was primarily ded-

icated to research activities (PGORI252), the submission of the paper entitled "A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems" [161] to the IEEE Access journal, a Qualis A3 journal according to the CAPES Sucupira platform, with the PhD candidate as the first author, and to the preparation of the PhD thesis. IEEE Access is a high-impact journal with a 2024 Impact Factor of 3.6 and a CiteScore of 9.8, indexed in Web of Science and Scopus. During this semester, an intellectual property registration was also filed with the INPI (National Institute of Industrial Property) under certificate number BR512025005202-2, titled "AI-Based Recipe Generator for Copper Thin-Film Deposition Equipment Using Sputtering" [216], issued on 21 October 2025.

The fifth semester of the PhD program (Semester 26.1) was dedicated to research activities (PGORI261) and to the preparation of the PhD thesis. This semester is planned to conclude the PhD program through the final examination, enabling the candidate to pursue new academic opportunities.

6.2 Contributions of This Thesis

This PhD thesis presents two major contributions that advance the scientific frontier in chaos-based cryptography (see Section 1.5). The first is a structured SLR encompassing the most recent primary studies in the area, focused on the use of chaos-based S-Boxes as encryption primitives. The second is a novel chaos-based S-Box, the CB-SBox, which employs OtF computations to enhance resistance against DAP and LAP attacks, while improving area and power efficiency. For ease of reference, these contributions are summarized in the last row of Tables 6.2 and 6.3. Specifically, Table 6.2 (related to [161]) presents the only literature review combining an SLR-type study (fourth column) with a focus on S-Boxes for block ciphers (third column). In turn, Table 6.3 (related to [180]) highlights the sole primary study answering “Yes” to the OtF criterion (third column).

Table 6.1: Schedule of Activities

<i>Doctoral Activities</i>	<i>24.1</i>	<i>24.2</i>	<i>25.1</i>	<i>25.2</i>	<i>26.1</i>
Linear Systems Theory (PGENE600)	C				
Real-Time Systems (PGENE537)	C				
Software and Systems Verification (PGENE549)	C				
Supervised Study I (PGENE614)	C				
Paper Submission to SBCCI 2024 Conference [196]	C				
Master's Degree Recognition (PGENE617)		C			
English Language Proficiency (PGENE599)		C			
Supervised Study II (PGENE615)		C			
Paper Submission to <i>Sensors</i> Journal [209]		C			
Supervised Study III (PGENE616)			C		
Bibliographic Research	C	C	C	C	C
Experiments and Simulations		C	C	C	C
Paper Submission to <i>SIoT</i> 2025 Conference [210]			C		
Paper Submission to <i>Electronics</i> Journal [180]			C		
Preparation of Qualification Document		C	C		
Qualification Exam			C		
Qualification Result (Approved)			C		
Research Activities (PGORI252)				C	
Intellectual Property Registration at INPI [216]				C	
Paper Submission to <i>IEEE Access</i> Journal [161]				C	
Research Activities (PGORI261)					C
Preparation of PhD Thesis				C	C
PhD Thesis Exam					P
PhD Thesis Exam Result					P

First letter: **C** — Completed, **A** — Active, **P** — Planned.

Table 6.2: Summary of Selected Stand-Alone Literature Reviews on Chaos-Based Cryptography

ID	Title	Application Area	Publisher	Review Type	RF	Time Frame	PG	CT	Gap	FW	Scr
2013 Sadkhan [140] Iraq	Chaos based cryptography for voice encryption in wireless communication	Voice Encryption	IEEE	Narrative	58	2001 to 2010	8	6	No	Yes	2
2013 Hussain [141] Pakistan	Literature survey on nonlinear components and chaotic nonlinear components of block ciphers	S-Box in Block Ciphers	Springer	Tutorial	73	2005 to 2011	36	17	No	No	2
2014 Zhen [142] China	A Survey of Chaos-Based Cryptography	None	IEEE	Narrative	79	1990 to 2014	8	10	No	Yes	2
2015 Shukla [143] India	Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems	Wired and Wireless Networks	MDPI	Survey	62	1993 to 2015	23	20	No	No	1
2016 Fang [144] China	A Survey on DCSK-Based Communication Systems and Their Application to UWB Scenarios	UWB Wireless Networks	IEEE	SOTA	176	1996 to 2015	34	46	No	Yes	4
2021 Muthu [145] India	Review of Chaos Detection Techniques in Image Encryption	Chaos Detection	Springer	Survey	99	2007 to 2020	24	8	Yes	No	5
2021 Khaleel [146] Iraq	Chaotic Image Cryptography Systems: A Review	Image Encryption	Other	Survey	49	2010 to 2020	14	3	No	Yes	2
2022 Haseeb [147] Iraq	A Survey on Speech Encryption Using Chaos Map	Voice Encryption	IEEE	Narrative	41	2018 to 2022	6	0	No	No	1
2022 Fang [148] China	A survey of image encryption algorithms based on chaotic system	Image Encryption	Springer	Survey	130	2010 to 2022	29	23	Yes	Yes	4
2022 Zia [149] UK	Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains	Image Encryption	Springer	Survey	165	2016 to 2021	19	53	Yes	Yes	4
2022 Zolfaghari [150] Japan	Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap	Image Encryption	MDPI	Survey	279	2014 to 2022	38	25	No	Yes	5
2022 Alhazaimeh [151] Jordan	Chaotic based multimedia encryption: a survey for network and internet security	Multimedia Encryption	Other	Narrative	31	2001 to 2022	9	8	No	No	2
2022 Shraida [152] Iraq	Chaotic-Based Color Image Encryption Algorithms: A Review	Color Image Encryption	Other	Survey	37	2017 to 2022	10	0	No	No	3
2023 Zhang [156] China	Chaos-Based Image Encryption: Review, Application, and Challenges	Image Encryption	MDPI	Survey	204	1996 to 2023	39	35	Yes	Yes	5
2024 Singh [157] India	A systematic literature review on chaotic maps-based image security techniques	Image Encryption	Elsevier	SLR	73	2006 to 2019	11	0	No	No	3
2025 Gupta [158] India	A survey on image cryptography mechanisms: hitherto, and future directions	Image Encryption	Elsevier	SOTA	134	2003 to 2025	24	0	Yes	Yes	5
2025 Zhang [159] China	Chaotic Image Security Techniques and Developments: A Review	Image Encryption	MDPI	Survey	171	1997 to 2025	28	0	No	No	4
2025 Dutra [161] Brazil	A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems	S-Box Block Ciphers	IEEE	SLR	170	1998 to 2025	30	0	Yes	Yes	5

NOTES - ID: Identification, including year of publication, first author, and country. Application Area: Main area of the work described in the paper. Review type: SLR, addressing specific research questions; SMS, maps broad research areas and identifies gaps; Survey, collects primary data, generating original quantitative or qualitative insights; Tutorial Review, explains concepts and techniques step-by-step; SOTA, summarizes the most recent advances and trends; Narrative Review, descriptive overview based on the author's judgment; and Not-a-Review (NoR), primary research, or case studies. RF: Number of References. PG: Number of pages. CT: Number of citations received according to <https://scite.ai/>. Gap (Yes or No): Does the paper describe research gaps? FW (Yes or No): Does the paper recommend future work? Scr (1 to 5): Paper score with 5 been the best.

Table 6.3: Systematic Review Table for Topics: Chaos, Encryption, and S-Boxes

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
1998 Kocarev [22] Macedonia Conference IEEE	4pg 8rf 15 15 23 25 years 7 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Partitioning the state space of the Hyperbolic chaotic map, and applied to a Feistel symmetric block cipher	No application domains are specified, it deals only with bits	No platforms HW/SW are specified, it deals only with the algorithm	S-Boxes are not part of this study	Counting number of bits changing for different plaintext of cipher keys
2001 Jakimoski [24] USA Journal IEEE	7pg 40rf 15 15 23 25 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	A 8-bit S-Box, based on the Logistic and Exponential chaotic maps, applied to a Feistel block cipher	No application domains are specified	Easy implementation (HW/SW) because it uses byte operations	Linear and differential probability bias; and bijectivity forced during construction	Preliminary results (not reported) indicate it has good cryptographic properties
2005 Tang [29] China Journal Elsevier	9pg 27rf 19 18 75 21 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = Yes	120 8-bit S-Boxes based in skew tent chaotic maps, obtained by changing IC and iteration time	No application domains are specified	No platforms HW/SW are specified	Bijectivity, Nonlinearity, SAC, BIC, Equiprobable input/outup XOR distribution	Criteria for good S-Boxes fulfilled implying immunity to resist differential cryptanalysis
2012 Peng [37] China Journal IGI Global	20pg 31rf 2 2 6 14 years 7 score 2 grade	4D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	500 key-dependent dynamic 8-bit chaotic S-Boxes generated using Hyperchaotic Lorenz System	Cognitive informatics, exemplified by digital image encryption	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC, DP_f	Histogram and correlation of 2000 pairs of horizontal adjacent pixels
2014 Guesmi [38] Tunisia Conference IEEE	7pg 33rf 26 26 46 12 years 7 score 3 grade	1D + 3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Logistic map for initial 8-bit S-Box and Lorenz chaotic system for genetic algorithm control parameters	No application domain are specified	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC	The cipher was neither implemented nor evaluated
2017 Rashmi [40] India Journal ISROSET	13pg 21rf 0 0 0 9 years 7 score 1 grade	2D + 2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Self adaptive image encryption technique based on Logistic and Arnold maps without S-Boxes	Image encryption by pixel permutation and diffusion	Intel(R) Pentium(R) 2.30 GHz with Matlab 7.0	The S-Box was neither implemented nor evaluated	Histogram, correlation, entropy, MSE, NPCR, PSNR, UACI, speed of encryption
2019 Khan [42] Pakistan Journal IEEE	12pg 59rf 25 25 27 7 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	SP-Network based on Gold Sequences and chaotic Logistic Tent systems using S-Box and P-Box	Color image encryption	No platforms HW/SW are specified	Nonlinearity, BIC, SAC, NPCR, UACI, Linear and Differential approximation probability	Histogram and adjacent pixel correlation analysis of 3 images (Lena, Baboon, and Pepper)
2020 Ahmad [43] India Journal IEEE	15pg 85rf 39 37 62 6 years 7 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hybrid-constructed S-Boxes (5–8 bit; 4×8 – 16×16) using Ahmad's improved chaotic map and algebraic group operations (MOD, SIN, and POWER)	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, nonlinearity, SAC, BIC-NL, LAP, DAP	Histogram and MLC
2020 Ibrahim [44] Saudi Arabia Journal IEEE	17pg 56rf 90 62 90 6 years 7 score 5 grade	2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	A hybrid of Block Cipher (PRNG MT 19937), Stream Cipher (chaotic maps: Baker, Henon or other) and 8-bit S-Box	Medical image encryption	JavaSE 1.8 virtual machine, Intel Core i7-4790, 3.6GHz, 32GB RAM	Bijectivity by construction, nonlinearity, BIC, SAC, Differential Uniformity, LAP	Histogram, correlation, entropy, NIST, texture, UACI, NPCR, CPA, CCA, key sensitivity, key space, speed

Continued on the next page

Table 6.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2020 Lidong [45] China Journal IEEE	18pg 58rf 37 12 37 6 years 7 score 5 grade	2D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hibrid encryption combining compression, 2D-LSCM chaos and 16 x 16 1D-STs-based S-Box	Image encryption	MATLAB 2018b, Intel(R) Core(TM) i7-8550U, 8G RAM, WIN 10 Enterprise	No S-Box evaluation	CPA, key space, key sensibility, histogram, correlation, entropy, noise and data loss, GLCM, time complexity
2020 Zou [46] China Journal IEEE	13pg 44rf 46 16 46 7 years 7 score 4 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Encryption with a improved (nonlinear kinetic complexity and ergodicity) of Lorenz system	Color Image encryption	No platforms HW/SW are specified	No S-Box was implemented	Key security, key space, correlation, entropy, DAP, noise attack, data loss
2021 Maadeed [47] Qatar Journal Springer	22pg 46rf 14 14 57 5 years 7 score 4 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Stream cipher, 16 novel static 8-bit polynomial S-Boxes, and a new chaotic encryption algorithm	Image encryption	MATLAB, Windows 10, i5 CPU, 8GB RAM	Bijectivity by construction, nonlinearity, BIC, SAC, LAP, DAP	Correlation, entropy, contrast, homogeneity, energy, key space, key sensitivity, NPCR, UACI, noise, data loss, LAP, DAP, speed
2021 Jun [48] China Journal IEEE	17pg 53rf 39 39 39 5 years 7 score 4 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Block Cipher, 10x25 Logistic-based S-Box, with a dynamic encryption step	Image encryption	MATLAB 2018a, AMD Ryzen 5, 2.10 GHz, 8GB RAM, WIN 10	Bijectivity by construction	Histogram, χ^2 , correlation, UACI, NPCR, LAP, DAP, entropy, noise (Gaussian, Salt, Pepper), data loss
2022 Manzoor [5] Pakistan Journal IEEE	11pg 60rf 21 21 38 4 years 7 score 4 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	New MAZa chaotic map for design of dynamic 16 x 16 S-Boxes using a heuristic method	No application domain are specified	Visual C#, Windows 8, Intel core i7 CPU, 2.2 GHz, 4GB RAM	Bijectivity by construction, nonlinearity, fixed points, SAC, BIC, LAP, DAP	Key space
2022 Nazir [50] Pakistan Journal IEEE	16pg 94rf 16 16 27 7 years 7 score 5 grade	4D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Hybrid DNA Encoding (Logistic map), Hash function, block cipher (Hyperchaos), and S-Boxes (16 x 16)	Color image (M x N) encryption	Matlab R2015a, Intel i7-1165G7, 4.7 GHz, 8 GB RAM, Windows 8	Nonlinearity and SAC	PSNR, MSE, NIST, key space, key sensitivity, DAP, NPCR, UACI, correlation, histogram, GLCM, entropy, CPA, MAE, noise, data loss
2023 Goswami [53] India Journal IEEE	4pg 13rf 2 2 5 3 years 7 score 4 grade	NA $K_S = \text{NA}$ $T_T = \text{NA}$ $OfF = \text{NA}$ Degrad = NA	Stream Cipher, 32x32 bits S-Box in boolean function (no LUT, no chaos), Key Generation, LFSR, FSM	4G LTE security applications, focusing on area, power, and efficiency	Implemented on FPGA Zynq ZC702	No S-Box evaluations are performed (only FPGA resources utilization)	No cipher evaluations are performed (no encryption was realized)
2023 Zhang [52] China Journal MDPI	23pg 49rf 1 1 7 3 years 7 score 4 grade	2D $K_S = \text{NA}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = Yes	PRNG, hyperchos-based 16 x 16 dynamic S-Box, hybrid with quantum randow walks	Image encryption and video authentication (future work)	No platforms HW/SW are specified	Bijectivity by construction (swapping), nonlinearity, SAC, BIC, DAP, LAP, security, etc.	No cipher evaluations are performed (no encryption was realized)

Continued on the next page

Table 6.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2024 Alabdullah [56] Saudi Arabia Journal IEEE	12pg 45rf 4 0 3 2 years 7 score 4 grade	5D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	Key Stream, 16 x 16 S-Box based on Delannoy numbers and Bashir's multiwing hyperchaotic system	Information security, data protection, and secure communica- tion (future work)	No platforms HW/SW are specified	Bijectivity by construction (Delannoy Numbers), nonlinearity, SAC, BIC, LAP, DAP	No cipher evaluations are performed (no encryption was realized)
2024 Ibrahim [57] Saudi Arabia Journal IEEE	12pg 37rf 4 0 4 2 years 7 score 5 grade	2D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	PRNG-based 12-bit key dependent S-Box, 2D Baker chaotic-based stream cipher	Medical image encryption	Java VM 1.8, Intel i7-8565U, 1.8 GHz, 12GB RAM	Bijectivity by construction (no further evaluation is provided)	Histogram, entropy, correlation, χ^2 , NPCR, UACI, key sensitivity, key space, CPA, speed
2021 Mohamed [173] Egypt Journal IEEE	23pg 68rf 42 42 54 5 years 6 score 5 grade	4D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	PRNG, 16 x 16 S-Box, Chen's hyperchaotic system, Choquet fuzzy integral, DNA sequences	Image encryption	CPU 3.0 GHz, 8GB RAM, Windows 10, MATLAB R2017b	MLC, entropy, correlation, energy, Homogeneity	Key sensitivity, histogram, NIST, χ^2 , information entropy, correlation, NPCR, UACI, PSNR, contrast, speed, robustness
2020 Ibrahim [175] Saudi Arabia Journal IEEE	14pg 83rf 44 43 77 6 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	PRNG, ECC, Henon chaotic map, 16 x 16 S-Box	Image encryption	CPU Core- i7-8565U 1.8 GHz, 12GB RAM, MATLAB	Bijectivity by construction, NL, LAP, DAP, SAC, BIC-SAC	Histogram, χ^2 , correlation, entropy, key and plaintext sensitivity, NPCR, UACI, BFA, CPA, CCA, speed
2022 Haq [178] India Journal IEEE	15pg 63rf 4 4 26 4 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	Symmetric cipher, 16 x 16 S-Box, PWLCM chaotic map, 2D cellular automata, algebraic structures	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, NL, DAP, LAP, SAC, BIC-NL, correlation	Histogram, MLC
2021 Ramzan [176] Pakistan Journal IEEE	24pg 51rf 16 16 40 5 years 4 score 4 grade	NA $K_S = \text{No}$ $T_T = \text{NA}$ $OfF = \text{No}$ Degrade = NA	SPN, ECC based S-Box, no chaos map is used	Image encryption	No platforms HW/SW are specified	Bijectivity by construction, NL, LAP, SAC, BIC, DAP	Key sace and sensitivity, NPCR, UACI, entropy, χ^2 , correlation, histogram, MSE, PSNR
2019 Yi [174] China Journal IEEE	12pg 23rf 38 38 87 7 years 5 score 5 grade	1D + 1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	Block cipher, Feistel network, 16 x 16 S-Box, compound and sinusoidal chaotic maps, Baker map, linear congruence generator	Wireless sensor networks	CC2430 SoC platform, 8051 MCU 32 MHz, 128K flash, 8K RAM	Bijectivity by construction, NL, SAC, BIC, LAP, DAP, MELP	Key space, 0 and 1 balance, entropy, NIST, diffusion and confusion analysis, speed and storage
2022 Tian [179] China Journal MDPI	25pg 78rf 12 12 32 4 years 5 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrade = No	16 x 16 S-Box, modified discrete chaotic map, Arnold transformation, DRPE	Image encryption	CPU i5-9400, 2.9 GHz, 16 GB RAM, Windows 7, MATLAB R2012b	Bijectivity by construction, NL, SAC, BIC, BIC-NL, BIC-SAC, LAP, DAP	Key space and sensibility, histogram, χ^2 , MSE, PSNR, correlation, NPCR, UACI, data loss, noise attack, entropy, speed

Continued on the next page

Table 6.3 – Continued from previous page

Bibliographic Identification	Bibliometric Information	Chaotic Details	Primitives Description	Application Domain	Platforms (HW/SW)	S-Box Evaluation	Cipher Evaluation
2021 Hernandez [177] Mexico Journal MDPI	25pg 40rf 5 5 13 5 years 5 score 5 grade	1D $K_S = \text{No}$ $T_T = \text{No}$ $OfF = \text{No}$ Degrad = No	Symmetric encryption, block cipher, ECC, Logistic map, PRNG	Color image encryption	Intel Core i3 7350k, 4.0 GHz, dual-core, 8 GB RAM, HD SATA 7200 RPM, Windows 10 Pro	NL, algebraic degree and immunity, balance, correlation, DAP, SNR, power analysis, transparency order, correlation, etc.	Entropy, correlation, χ^2 , NPCR, UACI, avalanche effect, CPA, KPA, key space and sensitivity, data loss, noise attack, speed
2025 Dutra [180] Brazil Journal MDPI	28pg 63rf 1 1 1 1 year 7 score 5 grade	3D $K_S = \text{No}$ $T_T = \text{Yes}$ $OfF = \text{Yes}$ Degrad = Yes	A 19-bit S-Box, based on the Sprott B chaotic system (analyzed for encryption application), and applied to a Feistel block cipher	Image and text encryption, applied to Feistel and Hash structures	Xilinx Spartan-3 FPGA, tested using System Generator for MATLAB	Area, power, and timing on FPGA; linear and differential bias computation; and bijectivity	Frequency, throughput, and FPGA resource usage; histogram analysis for image and text data

Note: **Bibliographic Identification:** Year of publication, first author's surname and reference, country, type of venue (Journal or Conference), publisher; **Bibliometric Information:** Number of pages and references, total citations, mentioning, citing publications (<https://scite.ai/>), age of publication in years, reviewer score, and final grade; **Chaotic details:** Dimensions of chaotic systems used, Keyspace computed from initial conditions (Yes/No), Transient Time calculated (Yes/No), On the Fly chaos computation during encryption (Yes/No), chaos degradation considered (Yes/No); **Primitives Description:** Cryptographic primitives (S-Box, PRNG, block cipher, stream cipher, hash, ECC), the description of the S-Box (size; chaos-based; algebraic; heuristic; none), the chaotic system, and hybrid technologies (DNA, AI, ML, Blockchain, Genetic) used; **Application Domain:** Area where the cryptographic scheme is applied (Military; Satellite; Medical, Image encryption; General-purpose; Other); **Platforms (HW/SW):** Platforms used for implementation and testing; **S-Box Evaluation:** Cryptographic metrics (nonlinearity, bijectivity, SAC, BIC, etc.) and security metrics (linear and differential attacks, etc.); **Cipher Evaluation:** Statistical (histogram, boxplot, scatter, heatmap), tests (chi-square, correlation, entropy, NIST/Diehard), and performance metrics (throughput, latency, memory usage). NA: Not Applicable

6.3 Future Work

Directions for future work can be found in Chapter 1 (Introduction), Subsection 1.6.1 (Beyond the Scope); in Chapter 3 (State-of-the-Art), Subsections 3.2.2 (SoS - Extraction of Relevant Information), and 3.4 (Chapter Conclusions – SOTA); as well as in Chapter 5 (Experimental Results), Subsection 5.6 (Chapter Conclusions – CB-SBox). These directions are reviewed and summarized in the following paragraphs.

Chapter 1, Subsection 1.6.1 (Beyond the Scope) delineates what is outside the scope of the present PhD thesis, thereby providing indirect suggestions for future work. It identifies three areas for further investigation: (i) quantitative and qualitative analysis of other chaotic systems and maps as candidates for chaos-based cryptography; (ii) application of the proposed CB-SBox in different contexts, such as hash functions and asymmetric ciphers; and (iii) evaluation of the proposed CB-SBox or its cipher implementations according to metrics including NL, χ^2 , SAC, BIC, BIC-SAC, BIC-NL, NPCR, UACI, NIST SP800-22, PSNR, MLC, CPA, KPA, CCA, BFA, among others.

Chapter 3 presents two literature reviews: a SoS and a SLR. Both extensively address future research directions: by examining existing surveys in the SoS and investigating primary studies in the SLR. According to Subsection 3.2.2 (SoS - Extraction of Relevant Information) and the SoS summary presented in Table 6.2, among the seventeen surveyed studies, eight (47%) did not discuss future research directions. Of the remaining nine works (53%) that did, six (66.67%) focused on image encryption, thus suggesting that most future works should also target this field. Consequently, Subsection 3.2.2 primarily points toward future research in image encryption, particularly hybrid approaches combining chaos theory with other techniques such as DNA, AI, and quantum cryptography.

Chapter 3 also addresses the SLR. In this context, Subsection 3.4 (Chapter Conclusions – SOTA) highlights that future research should focus on the analysis of initial condition selection, efficient hardware implementation, and the evaluation of multi-parameterized hyperchaotic systems. Addressing these challenges will advance the practical applicability of chaotic systems in modern cryptographic frameworks.

Chapter 5, Subsection 5.6 (Chapter Conclusions – CB-SBox), discusses six open research directions. The first concerns the correlation between the position of a group of ICs and dispersion time, a promising topic for further investigation. The second involves the implementation of a programmable Chaos-Based Substitution Box, where both the S-Box length (NOB) and the underlying chaotic system can be dynamically configured to enhance adaptability and security. Third, the methodology of [4] could be extended to other chaotic systems, including hyperchaotic or higher-dimensional ones, those with multiple attractors, or improved ergodicity. Systems with stronger ergodicity may reduce the LongRun parameter, increase encryption throughput, and flatten the histogram in Figure 5.15b, mitigating potential weaknesses in the proposed C-SBox. The fourth direction notes that non-bijective S-Boxes, such as the CB-SBox, are suitable only for specific primitives like the Feistel network used in this work. While Feistel networks ensure global reversibility even with non-bijective S-Boxes, hash functions deliberately employ non-invertible transformations to guarantee one-way behavior. Hence, the CB-SBox concepts could also support the design of hash functions. Fifth, this research assessed the CB-SBox’s resistance to linear and differential cryptanalysis, confirming that larger S-Box sizes improve security; future studies may explore alternative or tailored attack strategies. Finally, alternative S-Box implementation methods, such as logic gate designs, could be investigated to compare large-scale realizations with the proposed CB-SBox.

Bibliography

- [1] SPOTT, J., “Some simple chaotic flows”, *Physical Review E*, v. 50, n. 2, pp. R647–R650, 1994.
- [2] DUTRA, É., FINAMORE, W. A., GLESNER, M., et al., “Chaotic Equations Initial Conditions Analysis for Cryptography Applications.” In: *XXVII Simpósio Brasileiro de Telecomunicações (SBrT), SBrT2009*, p. 6, Sociedade Brasileira de Telecomunicações, 2009.
- [3] DUTRA, E. C. E. S. J., “Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives”, 2025, Dataset available in <https://zenodo.org/records/14967851>.
- [4] DUTRA, E., GLESNER, M., FINAMORE, W., et al., “Novel method of chaotic systems evaluation for implementations of encryption algorithms”. In: *Telecommunications (ICT), 2010 IEEE 17th International Conference on*, pp. 89–96, 2010.
- [5] MANZOOR, A., ZAHID, A. H., HASSAN, M. T., “A New Dynamic Substitution Box for Data Security Using an Innovative Chaotic Map”, *IEEE Access*, v. 10, pp. 74164–74174, 2022.
- [6] LORENZ, N. E., “Deterministic non-periodic flows”, *Journal of Atmospheric Science, Vol. 22, No 02*, v. 20, pp. 130 – 141, 1963.
- [7] RÖSSLER, O. E., “An equation for continuous chaos”, *Physics Letters A*, v. 57, n. 5, pp. 397–398, 1976.
- [8] MAY, R. M., “Simple mathematical models with very complicated dynamics”, *Nature*, v. 261, n. 5560, pp. 459–467, 1976.

- [9] SPROTT, J., LINZ, S., “Algebraically simple chaotic flows”, *International Journal of Chaos Theory and Applications*, v. 5, n. 2, pp. 1–20, 2000.
- [10] CHUA, L., *The genesis of Chua’s circuit*. Electronics Research Laboratory, College of Engineering, University of California, 1992.
- [11] LINZ, S., SPROTT, J., “Elementary chaotic flow”, *Physics Letters A*, v. 259, n. 3-4, pp. 240–245, 1999.
- [12] M.D., V., KARTHIKEYAN, A., ZIVCAK, J., et al., “Dynamical Behavior of a New Chaotic System with One Stable Equilibrium”, *Mathematics*, v. 9, n. 24, pp. 9, 2021.
- [13] AHMADI, A., VIJAYAN, V., NATIQ, H., et al., “A Novel Megastable Chaotic System with Hidden Attractors and Its Parameter Estimation Using the Sparrow Search Algorithm”, *Computation*, v. 12, n. 12, pp. 18, 2024.
- [14] CHIRIKOV, B., “Transient chaos in quantum and classical mechanics”, *Foundations of physics*, v. 16, n. 1, pp. 39–49, 1986.
- [15] DITTO, W., “Applications of chaos in biology and medicine”. In: *AIP Conference Proceedings*, v. 376, p. 175, 1996.
- [16] SOLÉ, R., GAMARRA, J., GINOVART, M., et al., “Controlling chaos in ecology: from deterministic to individual-based models”, *Bulletin of Mathematical Biology*, v. 61, n. 6, pp. 1187–1207, 1999.
- [17] CONTOPOULOS, G., *Order and chaos in dynamical astronomy*. Springer Verlag, 2002.
- [18] KELBER, K., FALK, T., GÖTZ, M., et al., “Discrete-time chaotic coders for information encryption. Pt. 2: continuous-and discrete-value realisation”, 1996.
- [19] GÖTZ, M., KELBER, K., SCHWARZ, W., “Discrete-time chaotic encryption systems. I. Statistical design approach”, *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, v. 44, n. 10, pp. 963–970, 1997.

- [20] DACHSELT, F., KELBER, K., SCHWARZ, W., “Discrete-time chaotic encryption systems. III. Cryptographical analysis”, *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, v. 45, n. 9, pp. 983–988, 1998.
- [21] BAPTISTA, M., “Cryptography with chaos”, *Physics Letters A*, v. 240, n. 1-2, pp. 50–54, 1998.
- [22] KOCAREV, L., JAKIMOSKI, G., STOJANOVSKI, T., et al., “From chaotic maps to encryption schemes”. In: *ISCAS '98. Proceedings of the 1998 IEEE International Symposium on Circuits and Systems (Cat. No.98CH36187)*, v. 4, *ISCAS-98*, pp. 514–517, IEEE, 1998.
- [23] ALVAREZ, E., FERNANDEZ, A., GARCIA, P., et al., “New approach to chaotic encryption”, *Physics Letters A*, v. 263, n. 4-6, pp. 373–375, 1999.
- [24] JAKIMOSKI, G., KOCAREV, L., “Chaos and cryptography: Block encryption ciphers based on chaotic maps”, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, v. 48, n. 2, pp. 163–169, 2001.
- [25] LI, S., ZHENG, X., MOU, X., et al., “Chaotic encryption scheme for real-time digital video”. In: *Real-Time Imaging VI, Proceedings of SPIE*, v. 4666, pp. 149–160, 2002.
- [26] WONG, K. W., “A fast chaotic cryptographic scheme with dynamic look-up table”, *Physics Letters A*, v. 298, n. 4, pp. 238–242, 2002.
- [27] WONG, K.-W., HO, S.-W., YUNG, C.-K., “A chaotic cryptography scheme for generating short ciphertext”, *Physics Letters A*, v. 310, n. 1, pp. 67–73, 2003.
- [28] WONG, K. W., “A combined chaotic cryptographic and hashing scheme”, *Physics letters A*, v. 307, n. 5-6, pp. 292–298, 2003.
- [29] TANG, G., LIAO, X., “A method for designing dynamical S-boxes based on discretized chaotic map”, *Chaos, Solitons and Fractals*, v. 23, n. 5, pp. 1901–1909, 2005.

- [30] TENNY, R., TSIMRING, L., “Additive mixing modulation for public key encryption based on distributed dynamics”, *Circuits and Systems I: Regular Papers, IEEE Transactions on*, v. 52, n. 3, pp. 672–679, 2005.
- [31] BOSE, R., PATHAK, S., “A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system”, *Circuits and Systems I: Regular Papers, IEEE Transactions on*, v. 53, n. 4, pp. 848–857, 2006.
- [32] LIAO, X., WONG, K., “Improving the security of a dynamic look-up table based chaotic cryptosystem”, *Circuits and Systems II: Express Briefs, IEEE Transactions on*, v. 53, n. 6, pp. 502–506, 2006.
- [33] XIANG, T., LIAO, X., TANG, G., et al., “A novel block cryptosystem based on iterating a chaotic map”, *Physics Letters A*, v. 349, n. 1-4, pp. 109–115, 2006.
- [34] WONG, K., YUEN, C., “Embedding compression in chaos-based cryptography”, *Circuits and Systems II: Express Briefs, IEEE Transactions on*, v. 55, n. 11, pp. 1193–1197, 2008.
- [35] CHEN, J., ZHOU, J., WONG, K., “A Modified Chaos-Based Joint Compression and Encryption Scheme”, *Circuits and Systems II: Express Briefs, IEEE Transactions on*, v. 58, n. 99, pp. 110–114, 2011.
- [36] PIRET, G., ROCHE, T., CARLET, C., “PICARO – A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance”, 2012.
- [37] PENG, J., ZHANG, D., LIAO, X., “A Novel Approach for Designing Dynamical S-Boxes Using Hyperchaotic System”, *International Journal of Cognitive Informatics and Natural Intelligence*, v. 6, n. 1, pp. 100–119, 2012.
- [38] GUESMI, R., BEN FARAH, M. A., KACHOURI, A., et al., “A novel design of Chaos based S-Boxes using genetic algorithm techniques”. In: *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pp. 678–684, IEEE: Doha, Qatar, 2014.

- [39] ZHANG, W., PASALIC, E., “Highly Nonlinear Balanced S-Boxes With Good Differential Properties”, *IEEE Transactions on Information Theory*, v. 60, n. 12, pp. 7970–7979, 2014.
- [40] RASHMI, B. D. P., R.K., B., PRABHAKAR, S., et al., “Performance Analysis of Self Adaptive Image Encryption Technique”, *International Journal of Scientific Research in Network Security and Communication*, v. 5, pp. 44–58, 6 2017.
- [41] ZHU, S., WANG, G., ZHU, C., “A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes”, *Entropy*, v. 21, n. 8, pp. 790, 2019.
- [42] KHAN, M. F., AHMED, A., SALEEM, K., et al., “A Novel Design of Cryptographic SP-Network Based on Gold Sequences and Chaotic Logistic Tent System”, *IEEE Access*, v. 7, pp. 84980–84991, 2019.
- [43] AHMAD, M., AL-SOLAMI, E., ALGHAMDI, A. M., et al., “Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures”, *IEEE Access*, v. 8, pp. 110397–110411, 2020.
- [44] IBRAHIM, S., ALHUMYANI, H., MASUD, M., et al., “Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps”, *IEEE Access*, v. 8, pp. 160433–160449, 2020.
- [45] LIDONG, L., JIANG, D., WANG, X., et al., “A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing”, *IEEE Access*, v. 8, pp. 210382–210399, 2020.
- [46] ZOU, C., ZHANG, Q., WEI, X., et al., “Image Encryption Based on Improved Lorenz System”, *IEEE Access*, v. 8, pp. 75728–75740, 2020.
- [47] AL-MAADEED, T. A., HUSSAIN, I., ANEES, A., et al., “A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes”, v. 80, pp. 24801–24822, 2021.
- [48] JUN, W. J., FUN, T. S., “A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step”, *IEEE Access*, v. 9, pp. 120596–120612, 2021.

- [49] FENG, W., ZHANG, J., QIN, Z., “A Secure and Efficient Image Transmission Scheme Based on Two Chaotic Maps”, *Complexity, Wiley*, v. 2021, n. 1, pp. 1–19, 2021.
- [50] NAZIR, H., BAJWA, I. S., ABDULLAH, S., et al., “A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes”, v. 10, pp. 14480–14495, 2022.
- [51] JASSIM, S., FARHAN, A., “Designing a Novel Efficient Substitution-Box by Using a Flower Pollination Algorithm and Chaos System”, v. 15, n. 1, pp. 176–187, 2022.
- [52] ZHANG, L., MA, C., ZHAO, Y., et al., “A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map”, *Mathematics*, v. 12, n. 1, pp. 84, 2023.
- [53] GOSWAMI, S. S. P., TRIVEDI, G., “FPGA Implementation of Modified SNOW 3G Stream Ciphers Using Fast and Resource Efficient Substitution Box”, *IEEE Embedded Systems Letters*, v. 15, n. 4, pp. 238–241, Dec 2023.
- [54] QIAN, K., XIAO, Y., WEI, Y., et al., “A Robust Memristor-Enhanced Polynomial Hyper-Chaotic Map and Its Multi-Channel Image Encryption Application”, *Micromachines*, v. 14, n. 11, pp. 25, 2023.
- [55] FENG, W., WANG, Q., LIU, H., et al., “Exploiting Newly Designed Fractional-Order 3D Lorenz Chaotic System and 2D Discrete Polynomial Hyper-Chaotic Map for High-Performance Multi-Image Encryption”, *Fractal and Fractional*, v. 7, n. 12, pp. 30, 2023.
- [56] ALABDUALLAH, B., BANGA, A., IQBAL, N., et al., “Advancing Cryptographic Security With a New Delannoy-Derived Chaotic S-Box”, v. 12, pp. 82926–82937, 2024.
- [57] IBRAHIM, S., ABBAS, A. M., ALHARBI, A. A., et al., “A New 12-Bit Chaotic Image Encryption Scheme Using a 12×12 Dynamic S-Box”, *IEEE Access*, v. 12, pp. 37631–37642, 2024.

- [58] FENG, W., YANG, J., ZHAO, X., et al., “A Novel Multi-Channel Image Encryption Algorithm Leveraging Pixel Reorganization and Hyperchaotic Maps”, *Mathematics*, v. 12, n. 24, pp. 27, 2024.
- [59] FENG, W., ZHANG, J., CHEN, Y., et al., “Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption”, *Expert Systems with Applications*, v. 246, 2024.
- [60] MA, X., WANG, Z., WANG, C., “An Image Encryption Algorithm Based on Tabu Search and Hyperchaos”, *International Journal of Bifurcation and Chaos*, v. 34, n. 14, 2024.
- [61] YU, F., ZHANG, S., SU, D., et al., “Dynamic Analysis and Implementation of FPGA for a New 4D Fractional-Order Memristive Hopfield Neural Network”, *Fractal and Fractional*, v. 9, n. 2, pp. 20, 2025.
- [62] SHANNON, C. E., “Communication theory of secrecy systems”, *The Bell System Technical Journal*, v. 28, n. 4, pp. 656–715, 1949.
- [63] ALVAREZ, G., LI, S., “Some basic cryptographic requirements for chaos-based cryptosystems”, *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, v. 16, n. 8, pp. 2129–2151, 2006.
- [64] ZHANG, D., “The Application of Data Encryption Technology in Computer Network Information Security”. In: *2023 International Conference on Applied Physics and Computing (ICAPC)*, pp. 379–384, IEEE, 2023.
- [65] ASSAD, S. E., LOZI, R., PUECH, W., (eds), *Cryptography and Its Applications in Information Security*. MDPI - Multidisciplinary Digital Publishing Institute, 2022.
- [66] LIU, H., “The application of data encryption technology in computer network system”, v. 9, n. 1, pp. 432, 2024.
- [67] LI, C., PRENEEL, B., “The Design of Stream Ciphers”, 2023.
- [68] ZHAO, Y., XUYANG, RANRANLI, “Design of Feedback Shift Register of Against Power Analysis Attack”, v. 58, n. 2, pp. 517–527, 2019.

- [69] MARK, “Securing implementations of feedback-shift-register-based ciphers using compiler optimizations and co-processors”, 2022.
- [70] KUMARI, R., PANDEY, J. G., KARMAKAR, A., “An RTL Implementation of the Data Encryption Standard (DES)”, 2023.
- [71] MOHAMMAD SHAH, I. N., ISMAIL, E. S., SAMAT, F., et al., “Modified Generalized Feistel Network Block Cipher for the Internet of Things”, v. 15, n. 4, pp. 900, 2023.
- [72] BAGHERI, N., SADEGHI, S., RAVI, P., et al., “SIPFA: Statistical Ineffective Persistent Faults Analysis on Feistel Ciphers”, , pp. 367–390 2022.
- [73] SALEM, I. E., SALMAN, A. M., MIJWIL, M. M., “A Survey: Cryptographic Hash Functions for Digital Stamping”, v. 54, n. 6, 2019.
- [74] TORADMALLE, D., SINGH, R., SHASTRI, H., et al., “Prominence Of ECDSA Over RSA Digital Signature Algorithm”. In: *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, pp. 253–257, Aug 2018.
- [75] PRENEEL, B., RIJMEN, V., (eds), *State of the Art in Applied Cryptography*. N. 1528, *Lecture Notes in Computer Science*, Springer, 1998, Course on Computer Security and Industrial Cryptography, Leuven, Belgium, June 3-6, 1997 Revised Lectures.
- [76] THAMMARAT, C., TECHAPANUPREEDA, C., “Secure Key Establishment Protocol for Smart Homes Based on Symmetric Cryptography”. In: *2022 International Conference on Information Networking (ICOIN)*, pp. 46–51, Jan 2022.
- [77] SCHNEIER, B., *Applied cryptography*. 20th ed. Wiley.
- [78] WU, Y., NOONAN, J. P., AGAIAN, S., “A novel information entropy based randomness test for image encryption”. In: *2011 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2676–2680, 2011.

- [79] MENEZES, A. J., *Handbook of Applied Cryptography*. First edition. ed. *Discrete Mathematics and Its Applications*, CRC Press,, Includes bibliographical references and index.
- [80] NAKAMOTO, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, <https://bitcoin.org/bitcoin.pdf>, 2008, Accessed: 2026-04-26.
- [81] ZHENG, Z., XIE, S., DAI, H. N., et al., “Blockchain challenges and opportunities: a survey”, v. 14, n. 4, pp. 352–375.
- [82] DE MORAES CRUZ, C. A., “Wall or Saturation?: Physical Constraints on Scaling Exact Computation”, Kindle eBook, 2025, Self-published via Amazon Kindle Direct Publishing.
- [83] KNIGHT, S., “This machine needs to be turned more times than there are atoms in the universe”, 2020.
- [84] WATSON, B., BARY, W. T. D., *Complete Works of Chuang Tzu*. Columbia University Press, 1968.
- [85] DUTRA E SILVA, E. C. J., *Analysis, Design and FPGA-Implementation of Chaotic Systems as Alternative for Gaussian Noise Generation*, Master’s Thesis, Technische Universität Darmstadt (TUD), 2004.
- [86] MAXWELL, J. C., *Theory of Heat*. Digitally printed version from the first ed. ed. *Cambridge library collection*, Cambridge University Press.
- [87] MAXWELL, J. C., *Maxwell*. Nachdr. der orig.-ausg. von 1890 ed., v. Vol. 1. Univ. Press, 2010.
- [88] POINCARÉ, H., *Science and Method*. Cosimo Classics, 2007.
- [89] MORSE, H. M., “Recurrent geodesics on a surface of negative curvature”, *Transactions of the American Mathematical Society*, v. 22, pp. 84–100, 1921.
- [90] BIRKHOFF, G. D., “Surface transformations and their dynamical applications”, v. 43, n. 0, pp. 1–119, 1922.

- [91] LEVINSON, N., “A Second Order Differential Equation with Singular Solutions”, v. 50, n. 1, pp. 127, 1949.
- [92] KOLMOGOROV, A. A. N., “On conservation of conditionally periodic motions for a small change in Hamilton’s function”, *Proceedings of the USSR Academy of Sciences*, v. 98, pp. 527–530, 1954.
- [93] ARNOLD, V. I., “Proof of a theorem of A. N. Kolmogorov on the preservation of conditionally periodic motions under a small perturbation of the Hamiltonian”, v. 18, n. 5, pp. 9–36, 1963.
- [94] MOSER, J., “On invariant curves of area-preserving mappings of an annulus”, , pp. 1–201962.
- [95] WALKER, G. H., FORD, J., “Amplitude Instability and Ergodic Behavior for Conservative Nonlinear Oscillator Systems”, v. 188, n. 1, pp. 416–432, 1969.
- [96] STEWART, I., *Does God play dice? the mathematics of chaos*. Blackwell Publishers, 1990.
- [97] LORENZ, E. N., *The Essence of Chaos*. [nachdr.] ed. *The @Jessie and John Danz Lectures*, Univ. of Washington Press, 2008.
- [98] VIJAYAKUMAR, M., AHILAN, A., “An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map”, v. 15, n. 4, pp. 15.
- [99] ALVAREZ, G., MONTROYA, F., ROMERA, M., et al., “Cryptanalysis of an ergodic chaotic cipher”, *Physics Letters A*, v. 311, n. 2-3, pp. 172–179, 2003.
- [100] STROGATZ, S. H., *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. 2nd ed. Westview Press, 2015.
- [101] EL-LATIF, A. A. A., RAMADOSS, J., ABD-EL-ATTY, B., et al., “A Novel Chaos-Based Cryptography Algorithm and Its Performance Analysis”, v. 10, n. 14.

- [102] TSAFACK, N., KENGNE, J., ABD-EL-ATTY, B., et al., “Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption”, v. 515, pp. 191–217.
- [103] FEIGENBAUM, M. J., “Quantitative universality for a class of nonlinear transformations”, v. 19, n. 1, pp. 25–52, 1978.
- [104] AHMAD, M., AL-SOLAMI, E., “Evolving Dynamic S-Boxes Using Fractional-Order Hopfield Neural Network Based Scheme”, v. 22, n. 7.
- [105] ALEXAN, W., ALEXAN, N., GABR, M., “Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs”, v. 7, n. 4.
- [106] BERIR, M., “A Fractional Study for Solving the Smoking Model and the Chaotic Engineering Model”. In: *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, pp. 1–6, IEEE, 2023.
- [107] YU, F., XU, S., LIN, Y., et al., “Design and Analysis of a Novel Fractional-Order System with Hidden Dynamics, Hyperchaotic Behavior and Multi-Scroll Attractors”, v. 12, n. 14, pp. 2227, 2024.
- [108] WOLF, A., SWIFT, J., SWINNEY, H., et al., “Determining Lyapunov exponents from a time series”, *Physica D: Nonlinear Phenomena*, v. 16, n. 3, pp. 285–317, 1985.
- [109] ECKMANN, J. P., RUELLE, D., “Ergodic theory of chaos and strange attractors”, v. 57, n. 3, pp. 617–656, 1985.
- [110] BREVITT, S., KLAGES, R., “Generalised Lyapunov stretching in a weakly chaotic open dynamical system”, v. 2839, n. 1, pp. 012013, 2024.
- [111] EUZZOR, S., DI GARBO, A., GINOUX, J.-M., et al., “Implementing Poincaré Sections for a Chaotic Relaxation Oscillator”, v. 67, n. 2, pp. 395–399, 2020.

- [112] SIMINOS, E., “Manifold learning of Poincaré sections reveals the topology of high-dimensional chaotic flows”, 2021.
- [113] INABA, N., NISHIO, Y., ENDO, T., “Chaos via torus breakdown from a four-dimensional autonomous oscillator with two diodes”, v. 240, n. 11, pp. 903–912, 2011.
- [114] APPERT, C., ERNST, M., “Chaos properties and localization in Lorentz lattice gases”, *Arxiv preprint chao-dyn/9705011*, 1997.
- [115] ASEERI, M., SOBHAY, M., LEE, P., “Lorenz chaotic model using filed programmable gate Array (FPGA)”. In: *Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on*, v. 1, pp. I–527, 2002.
- [116] LORENZ, E., “The mechanics of vacillation”, *J. Atmos. Sci.*, v. 20, n. 464, pp. 16–30, 1963.
- [117] BELAZI, A., RHOUMA, R., BELGHITH, S., “A novel approach to construct S-box based on Rossler system”. In: *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 611–615.
- [118] CHUA, L., LIN, G., “Canonical realization of Chua’s circuit family”, *Circuits and Systems, IEEE Transactions on*, v. 37, n. 7, pp. 885–902, 1990.
- [119] MADAN, R., *Chua’s circuit: a paradigm for chaos*. World Scientific Singapore, 1993.
- [120] AHMAD, M., AL-SOLAMI, E., “Improved 2D Discrete Hyperchaos Mapping with Complex Behaviour and Algebraic Structure for Strong S-Boxes Generation”, v. 2020, n. 1, pp. 16.
- [121] MUNYAEV, V. O., KHORKIN, D. S., BOLOTOV, M. I., et al., “Appearance of chaos and hyperchaos in evolving pendulum network”, v. 31, n. 6, 2021.
- [122] RÖSSLER, O. E., “An equation for hyperchaos”, *Physics Letters A*, v. 71, n. 2, pp. 155–157, 1979.

- [123] LEO KINGSTON, S., KAPITANIAK, T., DANA, S. K., “Transition to hyperchaos: Sudden expansion of attractor and intermittent large-amplitude events in dynamical systems.” *Chaos*, v. 32 8, n. 8, pp. 081106 – 081106, 2022.
- [124] ANKIT TIWARI, B. K. R., “Compound Chaotic Systems with Composite Attractors”, *World Scientific Journals*, v. 32, n. 09, 2022.
- [125] SINGH, R. K., MOHARIR, P. S., MARU, V. M., “Compound Chaos”, v. 06, n. 02, pp. 383–393, 1996.
- [126] LÜ, J., CHEN, G., ZHANG, S., “The compound structure of a new chaotic attractor”, *Chaos, Solitons & Fractals*, v. 14, n. 5, pp. 669–672, 2002.
- [127] HUANG, J.-H., LIU, Y., “A block encryption algorithm combined with the Logistic mapping and SPN structure”. In: *2010 2nd International Conference on Industrial and Information Systems*, v. 2, pp. 156–159.
- [128] MOHAMMED, R. S., “Simon Chaotic: An enhancement of SIMON block cipher by using Arnold and Henon chaotic maps”. In: *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, pp. 237–242.
- [129] QIU, J., LIAO, X., WANG, P., “A Method to Construct Dynamic S-box Based on Chaotic Map”. In: *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, v. 3, pp. 522–525.
- [130] YOUNES, QOBBI, ABDELLAH, et al., “An Image Encryption Algorithm Based on Substitution and Diffusion Chaotic Boxes”. In: *Artificial Intelligence and Smart Environment*, p. 184–190.
- [131] VINOTH, RAJ, SIVA, et al., “Reconfigurable color medical image encryptor using hardware accelerated Chao(S)-box triplets”, .
- [132] BASSEM, ABD, EL, et al., “A Novel Approach for Robust S-Box Construction Using a 5-D Chaotic Map and Its Application to Image Cryptosystem”. In: *Cybersecurity*.

- [133] CASSAL-QUIROGA., B. B., CAMPOS-CANTÓN, E., “Generation of Dynamical S-Boxes via Lag Time Chaotic Series for Cryptosystems”. In: *Complex Systems and Their Applications*.
- [134] XUANPING, ZHANG, YANBIN, et al., “An efficient chaotic image encryption based on alternate circular S-boxes”, , pp. 359–369 2014.
- [135] MUSHEER, AHMAD, HITESH, et al., “A Chaos Based Method for Efficient Cryptographic S-box Design”. In: *Security in Computing and Communications*, pp. 130–137, Springer Berlin Heidelberg, 2013.
- [136] AYAD, J., SAHIB HASAN, F., ALI, A., “OFDM Transmission for encrypted Images based on 3D Chaotic Map and S-Box through Fading Channel”. In: *2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)*, pp. 1–6.
- [137] YUAN, H., LUO, L., WANG, Y., “An S-box Construction Algorithm Based on Spatiotemporal Chaos”. In: *2010 International Conference on Communications and Mobile Computing*, v. 1, pp. 61–65.
- [138] KITCHENHAM, B., CHARTERS, S., *Guidelines for performing Systematic Literature Reviews in Software Engineering*, Tech. Rep. EBSE-2007-01, Keele University and University of Durham, 3 2007.
- [139] OKOLI, C., “A Guide to Conducting a Standalone Systematic Literature Review”, v. 37, n. 43, pp. 879 – 910, 2015.
- [140] SADKHAN, S. B., AL-SHERBAZ, A., MOHAMMED, R. S., “Chaos based cryptography for voice encryption in wireless communication”. In: *2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*, pp. 191–197, 2013.
- [141] HUSSAIN, I., SHAH, T., “Literature survey on nonlinear components and chaotic nonlinear components of block ciphers”, v. 74, n. 4, pp. 869–904, 2013.

- [142] ZHEN, P., ZHAO, G., MIN, L., et al., “A Survey of Chaos-Based Cryptography”. In: *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 237–244, IEEE, 2014.
- [143] SHUKLA, P. K., KHARE, A., RIZVI, M. A., et al., “Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing”, v. 17, n. 3, pp. 1387–1410, 2015.
- [144] FANG, Y., HAN, G., CHEN, P., et al., “A Survey on DCSK-Based Communication Systems and Their Application to UWB Scenarios”, v. 18, n. 3, pp. 1804–1837, 2016.
- [145] MUTHU, J. S., MURALI, P., “Review of Chaos Detection Techniques Performed on Chaotic Maps and Systems in Image Encryption”, v. 2, n. 5, pp. 392, 2021.
- [146] KHALEEL, A. H., ABDULJALEEL, I. Q., “Chaotic Image Cryptography Systems: A Review”, v. 3, n. 2, pp. 129–143, 2021.
- [147] HASEEB, E. H., KADHIM, S. A., MAHMOOD, A. S., “A Survey on Speech Encryption Using Chaos Map”. In: *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCITIT)*, pp. 248–253, IEEE, 2022.
- [148] FANG, P., LIU, H., WU, C., et al., “A survey of image encryption algorithms based on chaotic system”, v. 39, n. 5, pp. 1975–2003.
- [149] ZIA, U., MCCARTNEY, M., SCOTNEY, B., et al., “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains”, v. 21, n. 4, pp. 917–935.
- [150] ZOLFAGHARI, B., KOSHIBA, T., “Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap”, v. 5, n. 3, 2022.
- [151] AL-HAZAIMEH, O. M., ABU-EIN, A. A., AL-NAWASHI, M. M., et al., “Chaotic based multimedia encryption: a survey for network and internet security”, v. 11, n. 4, pp. 2151–2159, 2022.

- [152] SHRAIDA, G. K., YOUNIS, H. A., “Chaotic-Based Color Image Encryption Algorithms: A Review”, *Basrah Researches Sciences*, v. 48, n. 2, pp. 77–87, 2022.
- [153] SUNEJA, K., DUA, S., DUA, M., “A Review of Chaos based Image Encryption”. In: *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 693–698.
- [154] AYAD, J., HASAN, F. S., ALI, A. H., et al., “Image Encryption using Chaotic Techniques: A Survey Study”. In: *2021 International Conference in Advances in Power, Signal, and Information Technology (APSIT)*, pp. 1–6.
- [155] BU, Y., “Overview of Image Encryption Based on Chaotic System”. In: *2021 2nd International Conference on Computing and Data Science (CDS)*, pp. 100–103, IEEE.
- [156] ZHANG, B., LIU, L., “Chaos-Based Image Encryption: Review, Application, and Challenges”, v. 11, n. 11, pp. 2585, 2023, Cited by: 146; All Open Access, Gold Open Access.
- [157] SINGH, D., KAUR, S., KAUR, M., et al., “A systematic literature review on chaotic maps-based image security techniques”, v. 54, pp. 100659, 2024.
- [158] GUPTA, T., SELWAL, A., SHARMA, A. K., “A survey on image cryptography mechanisms: hitherto, and future directions”, v. 58, pp. 100783.
- [159] ZHANG, H., FENG, X., SUN, J., et al., “Chaotic Image Security Techniques and Developments: A Review”, *Mathematics*, v. 13, n. 12, 2025.
- [160] JADOON, S., PAN, L., HUDA, S., et al., “A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms”, v. 85, n. 3, pp. 41, 2026.
- [161] E SILVA JUNIOR, E. C. D., DE MORAES CRUZ, C. A., DA SILVA JUNIOR, P. F., et al., “A Systematic Literature Review on the Application of Chaos Theory to the Design of Substitution Boxes for Cryptographic Systems”, Manuscript under review after initial reviewer feedback.

- [162] DUTRA E SILVA, E., INDRUSIAK, L., GLESNER, M., “Advantages of the Linz-Sprott weak nonlinearity on the FPGA implementation of chaotic systems: a comparative analysis”. In: *Signals, Circuits and Systems, 2005. ISSCS 2005. International Symposium on*, v. 2, pp. 753–756, 2005.
- [163] ACIKKAPI, M. S., OZKAYNAK, F., “A Method to Determine the Most Suitable Initial Conditions of Chaotic Map in Statistical Randomness Applications”, v. 9, pp. 1482–1494.
- [164] WEN, J., FENG, Y., TAO, X., et al., “Dynamical Analysis of a New Chaotic System: Hidden Attractor, Coexisting-Attractors, Offset Boosting, and DSP Realization”, v. 9, pp. 167920–167927, 2021.
- [165] LI, S., *Analyses and New Designs of Digital Chaotic Ciphers*, PhD thesis, Xi'an Jiaotong University, 2003, Doctoral dissertation.
- [166] BAO, H., LI, H., HUA, Z., et al., “Sine-Transform-Based Memristive Hyperchaotic Model With Hardware Implementation”, v. 19, n. 3, pp. 2792–2801.
- [167] MATTHEWS, R., “On the Derivation of a Chaotic Encryption Algorithm”, v. 13, n. 1, pp. 29–42.
- [168] CHEN, G., CHEN, Y., LIAO, X., “An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps”, v. 31, n. 3, pp. 571–579, 2007.
- [169] EL-RAMLY, S., EL-GARF, T., SOLIMAN, A., “Dynamic generation of s-boxes in block cipher systems”. In: *Proceedings of the Eighteenth National Radio Science Conference. NRSC'2001 (IEEE Cat. No.01EX462)*, v. 2, NRSC-01, pp. 389–397, Acad. Sci. Res. & Technol, 2001.
- [170] MILLER, F., VANDOME, A., JOHN, M., *Fisher-Yates Shuffle*. VDM Publishing, 2010.
- [171] ZHANG, Y.-Q., HAO, J.-L., WANG, X.-Y., “An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map”, v. 8, pp. 54175–54188.

- [172] WEBSTER, A. F., TAVARES, S. E., “On the Design of S-Boxes”. In: *Advances in Cryptology — CRYPTO ’85 Proceedings*, pp. 523–534, Springer Berlin Heidelberg: Berlin, Heidelberg, 1986.
- [173] MOHAMED, A. G., KORANY, N. O., EL-KHAMY, S. E., “New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps”, v. 9, pp. 14284–14305.
- [174] YI, L., TONG, X., WANG, Z., et al., “A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network”, v. 7, pp. 53079–53090.
- [175] IBRAHIM, S., ALHARBI, A., “Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography”, v. 8, pp. 194289–194302.
- [176] RAMZAN, M., SHAH, T., HAZZAZI, M. M., et al., “Construction of S-Boxes Using Different Maps Over Elliptic Curves for Image Encryption”, v. 9, pp. 157106–157123.
- [177] HERNÁNDEZ-DÍAZ, E., PÉREZ-MEANA, H., SILVA-GARCÍA, V., et al., “JPEG Images Encryption Scheme Using Elliptic Curves and A New S-Box Generated by Chaos”, v. 10, n. 4.
- [178] HAQUE, A., ABDULHUSSEIN, T. A., AHMAD, M., et al., “A Strong Hybrid S-Box Scheme Based on Chaos, 2D Cellular Automata and Algebraic Structure”, v. 10, pp. 116167–116181.
- [179] TIAN, P., SU, R., “A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding”, v. 22, n. 14, pp. 25.
- [180] DUTRA E SILVA JUNIOR, É. C., CRUZ, C. A. D. M., SARAIVA, I. A. L., et al., “Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives”, *Electronics*, v. 14, n. 11, pp. 27, 2025.

- [181] UNITED NATIONS, DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, POPULATION DIVISION, “World Population Prospects 2022”, 2022.
- [182] BORNMANN, L., MUTZ, R., “Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references”, v. 66, n. 11, pp. 2215–2222.
- [183] MDPI, “MDPI Annual Report 2025”, mdpi.com/annual-report-2025, 2025, Accessed: 2026-05-03.
- [184] NÄTHER, C., HERZINGER, D., GAZDAG, S.-L., et al., “Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review”, v. 12, pp. 132107–132126.
- [185] TANG, L., LV, H., YANG, F., et al., “Complexity testing techniques for time series data: A comprehensive literature review”, v. 81, pp. 117–135.
- [186] HAMIDOUCHE, B., GUESMI, K., ESSOUNBOULI, N., “Mastering chaos: A review”, v. 58, pp. 100966.
- [187] JARJAR, M., HRAOUI, S., NAJAH, S., et al., “A New image encryption technology implementing a big random S-Box”. In: *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, pp. 1–6.
- [188] BECHEIKH, R., MANNAI, O., RHOUMA, R., et al., “A Novel Family of Strong S-Box Based on Ikeda Map and T-Function”. In: *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 475–481.
- [189] WANG, Y., YANG, L., LI, M., et al., “A method for designing S-box based on chaotic neural network”. In: *2010 Sixth International Conference on Natural Computation*, v. 2, pp. 1033–1037.
- [190] ALZAIDI, A. A., AHMAD, M., DOJA, M. N., et al., “A New 1D Chaotic Map and β -Hill Climbing for Generating Substitution-Boxes”, v. 6, pp. 55405–55418.

- [191] DAMASCENO, K., CRUZ, C., DE OLIVEIRA, A., et al., “Alternative N-bit Key Data Encryption for Block Ciphers”. In: *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2019)*, *SBSeg*, pp. 409–414, Sociedade Brasileira de Computação, 2019.
- [192] HEYS, H. M., “A tutorial on linear and differential cryptanalysis”, *XXVI Cryptologia*, v. 3, pp. 189–221, 2002.
- [193] RUELLE, D., TAKENS, F., “On the nature of turbulence”, *Communications in mathematical physics*, v. 20, n. 3, pp. 167–192, 1971.
- [194] MATSUI, M., “Linear cryptanalysis method for DES cipher”. In: *Advances in Cryptology—EUROCRYPT’93*, pp. 386–397, 1994.
- [195] BIHAM, E., SHAMIR, A., “Differential cryptanalysis of DES-like cryptosystems”, *Journal of cryptology*, v. 4, n. 1, pp. 3–72, 1991.
- [196] YOJO, L. S., SANTOS, F. G., ETCHEVERRY, L. P., et al., “A frugal integrated circuit packaging for non-planar surface-conformant electronics applications”. In: *2024 38th Symposium on Microelectronics Technology and Devices (SBMicro)*, pp. 1–4, IEEE, 2024.
- [197] YOJO, L. S., SANTOS, F. G., PONTES, F. B., et al., “Reliability Aspects and Study of Copper Seed Deposition on Polyimide via Sputtering”. In: *2023 37th Symposium on Microelectronics Technology and Devices (SBMicro)*, pp. 1–4, IEEE, 2023.
- [198] GREIG, W., “Integrated Circuit Packaging, Assembly and Interconnections”, , pp. 1–2962007.
- [199] EGITTO, F., DAS, R., MARCONI, F., et al., “Development of Electronic Substrates for Medical Device Applications”, v. 2012, pp. 001527–001546, 2012.
- [200] GUPTA, S., NAVARAJ, W., LORENZELLI, L., et al., “Ultra-thin chips for high-performance flexible electronics”, v. 2, 2018.

- [201] CORDEIRO, L., FISCHER, B., MARQUES-SILVA, J., “SMT-Based Bounded Model Checking for Embedded ANSI-C Software”, v. 38, n. 4, pp. 957–974.
- [202] BARRETO, R., CORDEIRO, L., FISCHER, B., “Verifying Embedded C Software with Timing Constraints Using an Untimed Bounded Model Checker”. In: *2011 Brazilian Symposium on Computing System Engineering*, pp. 46–52, IEEE.
- [203] BRENGUIER, R., CORDEIRO, L., KROENING, D., et al., “JBMC: A Bounded Model Checking Tool for Java Bytecode”, .
- [204] TIKHOMIROV, S., VOSKRESENSKAYA, E., IVANITSKIY, I., et al., “SmartCheck: Static Analysis of Ethereum Smart Contracts”. In: *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 9–16.
- [205] FEIST, J., GRIECO, G., GROCE, A., “Slither: A Static Analysis Framework for Smart Contracts”. In: *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 8–15, IEEE.
- [206] LUU, L., CHU, D.-H., OLICKEL, H., et al., “Making Smart Contracts Smarter”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS’16*, pp. 254–269, ACM.
- [207] SONG, K., MATULEVICIUS, N., DE LIMA FILHO, E. B., et al., “ESBMC-solidity: an SMT-based model checker for solidity smart contracts”. In: *Proceedings of the ACM/IEEE 44th International Conference on Software Engineering: Companion Proceedings, ICSE ’22*, pp. 65–69, ACM.
- [208] SHARMA, N., SHARMA, S., “A Survey of Mythril, A Smart Contract Security Analysis Tool for EVM Bytecode”, v. 13, pp. 51003–51010.
- [209] SOUZA, A. K. P., CRUZ, C. A. D. M., JUNIOR, E. C. D. E. S., et al., “Current Mirror Improved Potentiostat (CMIPot) for a Three Electrode Electrochemical Cell”, v. 24, n. 18, pp. 5897, 2024.

- [210] HENRRIQUE SANTOS, ISAIAS A. L. SARAIVA, E. C. D. E. S. J., “A Novel Wi-Fi Independent Wireless NetworkArchitecture for Industry 4.0 and IIoT Applications”, .
- [211] DUONG, P.-P., PHAM, C.-K., “Constructing 8×8 S-Boxes with Optimal Boolean Function Nonlinearity”, v. 9, n. 4, pp. 24, 2025.
- [212] RASHIDI, B., “Construction of Lightweight 6-Bit and 12-Bit S-Boxes With Low Hardware Complexity”, .
- [213] YASIN, G., KANVAL, A., SHOAIB, M., “Novel Chaos-Based S-box Constructions for Lightweight Encryption in IoT and Resource-Constrained Devices”, v. 4, n. 1, pp. 133–141.
- [214] LI, J., SUN, L., LIN, C., et al., “SED-UAV: A Synergistic Framework of Lightweight Chaotic Encryption and Multiscale Feature Detection for Secure UAV Applications”, v. 13, n. 5, pp. 8050–8063.
- [215] MOZAFARI, F., AHMADI, M., “Design and Implementation of a Low-Power Memristor-Based Piccolo-80 Lightweight Encryption Algorithm Using VTM Logic Gates”, v. 49, n. 1, pp. 25–38, 2026.
- [216] CARREIRA, W. H., NOGUEIRA, W. M. S., SARAIVA, I. A. L., et al., “Gerador de receitas por IA para equipamento de deposição de filmes finos de cobre por sputter”, Certificado de Registro de Programa de Computador, 10 2025, Válido por 50 anos a partir de 01/01/2024, conforme §2º, art. 2º da Lei 9.609/1998. Data de criação: 01/06/2023. Data de publicação: 01/09/2023. Titular: SENAI. Linguagens: HTML, JavaScript, Python, PHP, MySQL, CSS. Algoritmo hash (SHA-256): a35cf72672def4f2bb38e46c0f023192206ed4be3ba71c1f5165e0d715dd4c03.