الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

وزارة التعليم العالي والبحث العلمي

Ministry of Higher Education and Scientific Research

جامعة الشهيد الشيخ العربي التبسي

تبسة

Echahid Cheikh Larbi Tebessi University – Tebessa

Faculty of Science and Technology

Department of Electronic and Telecommunications

MASTER'S THESIS



Presented for obtaining the **Academic Master's degree**

Field: Telecommunications

Specialty: Network and Telecommunications

THEME

Secure free space optical communication based on chaotic key

Presented by:

- Salsabil HARRACHE
- Soundes CHANBI

Presented and evaluated, on 11/ 06/ 2025, In front of the jury:

Mr.	Lotfi HOUAM	MCB	Chair
Mrs.	Hanane DJELLAB	MCA	Supervisor
Mr.	Karim FERROUDJI	MCB	Reviewer


بسم الله الرحمن الرحيم

Acknowledgements

Above all, we humbly thank God for granting us the strength, patience, and perseverance to complete our studies and this thesis. His guidance has been our source of hope through every challenge we faced during this journey.

We are deeply grateful to our supervisor, **Dr.Djellab Hanane**, for her unwavering support, insightful advice, and constant encouragement. Her guidance throughout this work has been a cornerstone of our progress, and we are truly thankful for her time, dedication, and trust.

Our sincere thanks also go to **Dr. Menaa Saber**, whose input and collaboration made a meaningful impact on the development of this thesis. His readiness to help and thoughtful feedback were invaluable to us.

We would like to warmly thank **Ms. Alaoua Oumaima** and **Mr. Belhocine Yassin** for their generous help, technical support, and the time they dedicated to assisting us. Their involvement contributed significantly to the completion of this work.

Our appreciation extends to the **Faculty of Science and Technology**, especially the **Department of Electronics and Telecommunications**, for the knowledge and academic environment they provided. The quality of education and the professionalism of the staff have played a major role in our formation.

We also wish to express our gratitude to the members of the thesis committee for agreeing to evaluate our work and for their valuable time and remarks.

Finally, we reserve our deepest thanks for our families—our parents, siblings, and loved ones—who stood by us with love, patience, and encouragement. Their belief in us has been the driving force behind every achievement.

To all our friends who supported and motivated us during this period: thank you for being there. Your presence made this journey less difficult and more meaningful.

Dedication

First and foremost, I want to thank ALLAH the Almighty for granting me health, willpower, courage, and patience to complete my training and carry out this research work.

I wholeheartedly dedicate this work to:

To my father, Mokdad the solid pillar of our home, who has been by my side since my very first day of school until now.

To my mother, Fadila my constant light, who gave me unconditional love and whose prayers surrounded me like a protective shield throughout my journey.

o my brother, Fakher Eddine, whose unwavering support and strength guided me through every difficult turn.

To my sisters, Basma, who offered me her comforting smile, and Amina, for her strength and serenity that deeply inspired me.

To my friends, Fella and Nousaiba your presence comforted me during hard times, your kindness kept me from feeling alone, and you embodied the true meaning of friendship.

To my thesis partner, soundes thank you for your strength and dedication throughout this shared academic journey.

And to my supervisor, Ms. Hanane Djellab – your guidance, patience, and encouragement were invaluable. This work carries the mark of your mentorship.

SALSABIL

Dedication

First and foremost, I want to thank ALLAH the Almighty for granting me health, willpower, courage, and patience to complete my training and carry out this research work.

I wholeheartedly dedicate this work to:

To my father, Mohammed Lyazid – a source of strength who instilled courage and wisdom in me,

To my mother, Hassina – whose prayers, patience, and love guided me throughout.

To my supportive brothers, Sofiane, Salim, Karim, and Aymen – your presence gave me strength and confidence.

To my beloved sisters, Zina, Israa, Farah, Bouchra, and Manel – your love and joy brought light and color to my days.

To my dear friends – your companionship was a true comfort during hardship and success alike.

To my thesis partner, Salsabil – thank you for your strength and dedication throughout this shared academic journey.

And to my supervisor, Ms. Hanane Djellab – your guidance, patience, and encouragement were invaluable. This work carries the mark of your mentorship.

SOUNDES

Abstract

This thesis presents the simulation and validation of a secure Free Space Optical (FSO) communication system, tailored for next-generation 5G networks. To overcome the inherent vulnerabilities of FSO links—such as atmospheric interference—a chaos-based encryption technique is proposed, leveraging Chua's circuit for dynamic key generation. A technical analysis of FSO and 5G technologies highlights their key advantages, including high data throughput, low latency, and immunity to electromagnetic interference, while also addressing the challenges associated with their deployment. Chaotic encryption stands out as a promising solution due to its strong nonlinearity, sensitivity to initial conditions, and low computational complexity, making it particularly well-suited for physical-layer security. Cryptographic evaluation confirms high entropy (0.99943), strong sensitivity (MSE = 0.518), and a vast key space ($\sim 2^{131}$). The presence of a positive Lyapunov exponent ($\lambda_1 \approx 0.648$) further validates the chaotic behavior of the system. The system is validated through simulations using MATLAB and OPTISYSTEM under various operational conditions: data rates from 1 to 10 Gbps, distances up to 1.5 km, and atmospheric attenuations up to 8 dB/km. The results demonstrate excellent performance, maintaining a Bit Error Rate (BER) below 10^{-6} and outperforming non-secure configurations in terms of signal integrity, Q-factor, and eye diagram analysis. Overall, this study shows that chaos-based encryption is a secure, high-performance, and scalable solution for future 5G optical wireless infrastructures.

Keywords: Free Space Optics (FSO), 5G Networks, Chaotic Encryption, Chua Circuit, Bit Error Rate (BER)

Résumé

Ce mémoire présente la simulation et la validation d'un système de communication optique en espace libre (FSO) sécurisé, adapté aux réseaux 5G de nouvelle génération. Afin de pallier les vulnérabilités inhérentes aux liaisons FSO — telles que les interférences atmosphériques — une technique de chiffrement basée sur le chaos est proposée, exploitant le circuit de Chua pour la génération dynamique de clés. Une analyse technique des technologies FSO et 5G met en évidence leurs avantages, notamment un débit élevé, une faible latence et une immunité aux interférences électromagnétiques, tout en abordant les défis liés à leur déploiement. Le chiffrement chaotique s'impose comme une solution prometteuse grâce à sa forte non-linéarité, sa sensibilité aux conditions initiales et sa faible complexité de calcul, le rendant particulièrement adapté à la sécurité de la couche physique. L'évaluation cryptographique confirme une entropie élevée (0,99943), une forte sensibilité (MSE = 0,518), ainsi qu'un vaste espace de clés ($\sim 2^{131}$). La présence d'un exposant de Lyapunov positif ($\lambda_1 \approx 0{,}648$) valide également le comportement chaotique du système.

Le système est validé par des simulations sous MATLAB et OptiSystem dans des conditions opérationnelles variées : débits de 1 à 10 Gbps, distances allant jusqu'à 1,5 km et atténuations atmosphériques jusqu'à 8 dB/km. Les résultats révèlent d'excellentes performances, avec un taux d'erreur binaire (BER) inférieur à 10^{-6}, surpassant les configurations non sécurisées en termes d'intégrité du signal, de facteur Q et d'analyse des diagrammes de l'œil. Dans l'ensemble, cette étude démontre que le chiffrement basé sur le chaos constitue une solution à la fois sécurisée, performante et évolutive pour les futures infrastructures optiques sans fil de la 5G.

Mots clés : Optique en espace libre (FSO), Réseaux 5G, Chiffrement chaotique, Circuit de Chua, Taux d'erreur binaire (BER).

ملخص

تقدم هذه المذكرة محاكاة والتحقق من صحة نظام اتصالات ضوئي آمن للفضاء الحر (FSO)، تم تكييفه مع شبكات الجيل الخامس من الجيل الجديد. من أجل تجاوز نقاط الضعف الكامنة في وصلات FSO — مثل التداخلات الجوية — تم اقتراح تقنية تشفير قائمة على الفوضى، مستغلةً دائرة Chua لتوليد المفاتيح الديناميكية. يسلط التحليل التقني لتقنيتي FSO و5G الضوء على مزاياهما، بما في ذلك معدل نقل بيانات مرتفع، وزمن استجابة منخفض، ومناعة ضد التداخلات الكهرومغناطيسية، مع التطرق إلى التحديات المرتبطة بنشرهما. يُعتبر التشفير الفوضوي حلاً واعداً بفضل لاخطّيته القوية، وحساسيته العالية للظروف الابتدائية، وانخفاض تعقيده الحسابي، مما يجعله ملائماً بشكل خاص لأمن الطبقة الفيزيائية. تؤكد التقييمات التشفيرية وجود إنتروبيا عالية (0.99943)، وحساسية قوية MSE) (0.518 =، ومساحة مفاتيح ضخمة (2^{131}). كما تُثبت قيمة أس ليابونوف الموجبة ($\lambda_1 \approx 0.648$) السلوك الفوضوي للنظام. تم التحقق من أداء النظام من خلال محاكاة باستخدام برنامجي MATLAB وOptiSystem ضمن ظروف تشغيلية متنوعة: معدلات نقل بين 1 10 Gbps، ومسافات تصل إلى 1.5، وتوهين جوي يصل إلى 8. dB/km أظهرت النتائج أداءً ممتازاً مع معدل خطأ في البتات (BER) أقل من 10^{-6}، متفوقاً على الأنظمة غير المؤمّنة من حيث سلامة الإشارة، ومعامل Q، وتحليل مخططات العين (Eye Diagram). بشكل عام، تُظهر هذه الدراسة أن التشفير القائم على الفوضى يمثل حلاً آمناً، عالي الأداء، وقابلاً للتوسّع لبُنى الاتصالات البصرية اللاسلكية المستقبلية لشبكات 5G.

الكلمات المفتاحية: الاتصالات البصرية في الفضاء الحر (FSO)، شبكات الجيل الخامس (5G)، التشفير الفوضوي، دائرة Chua، معدل خطأ البت (BER)،

Contents

List of Figures **XI**

List of Tables **XIII**

List of Abbreviations **XIV**

General introduction **1**

1 Fundamentals of 5G Networks and FSO communications **3**

1.1 Introduction 3

1.2 Free Space Optic (FSO) communications systems 4

1.2.1 Definition 4

1.2.2 Key Features 5

1.2.3 Applications 5

1.2.4 Components of FSO Systems 6

1.2.5 Challenges 13

1.2.6 Comparison with Fiber Optic and Free Space Optical Communication 16

1.3 5G Networks 17

1.3.1 Definition 17

1.3.2 Key Features 17

1.3.3 Applications 18

1.3.4 Challenges 20

1.3.5 Architecture 21

1.4 Integration FSO communication in 5G networks 23

1.4.1 Conclusion 25

2 Chaotic approach for securing FSO systems **26**

2.1 Introduction 26

2.2 Encryption Techniques 27
2.2.1 Symmetric 27
2.2.2 Asymmetric 28
2.3 Adaptation of Encryption techniques to Free Space Optical systems Constraints Related to Optical Performance 29
2.3.1 The Choquet Fuzzy Integral (CFI) and integer wavelet transform (IWT) 30
2.3.2 Quantum Key Distribution (QKD) 30
2.3.3 Physical Layer Security (PLS) 31
2.3.4 Chaotic method 31
2.4 Comparison of different encryption methods 32
2.5 Chaotic Dynamical Systems 33
2.5.1 Dynamic System 33
2.5.2 Chaotic System 34
2.5.3 Properties 34
2.5.4 Chaos Vs Randomness 35
2.5.5 Mathematical Models of Chaos 35
2.5.6 Application of chaos to cryptography 40
2.6 Comparison between Classical Algorithms and Chaotic Encryption 41
2.7 Advantages and challenges of chaotic encryption in FSO systems 42
2.8 Conclusion 43

3 Design and Simulation of secure FSO system 45

General conclusion 46

Bibliography 48

List of Figures

1.1 The FSO System 4
1.2 Free Space Optics (FSO) links are employed to enable 5G connectivity within smart city networks 6
1.3 FSO Communication 6
1.4 block diagram of Transmitter side in FSO system 7
1.5 Laser diodes are modulated directly by varying the injection current 8
1.6 Laser diode using external modulation 9
1.7 Operating Principle of the Integrated Mach-Zehnder Modulator 10
1.8 Semiconductor Optical Amplifiers (SOAs) 10
1.9 Block diagram of the Receiver side in FSO systems 11
1.10 Propagation Channel in FSO system 12
1.11 Atmospheric medium between the transmitter and receiver in FSO communication systems 13
1.12 Effects of various physical and weather conditions on the FSO 15
1.13 Laser beam misalignment between FSO transceivers 16
1.14 Autonomous-driving in the Context of 5G Networks 19
1.15 Human-machine interface in 5G environments 19
1.16 Smart healthcare in the context of 5G 20
1.17 5G RAN Network 21
1.18 5G Core Network 22
1.19 5G Architecture Backhaul /Fronthaul 23
1.20 Integration of FSO in 5G Architecture 24
1.21 FSO link across multiple domains 25

2.1 Symmetric cryptography 27
2.2 Asymmetric cryptography 28
2.3 Block diagram of chaotic method 32

2.4 butterfly effect 34
2.5 Chua's Circuit 37
2.6 Characteristic of NR resistor 38

List of Tables

1.1 Comparison between FSO and fiber optic 16
1.2 Key Features of 5G 18

2.1 Comparison between some encryption techniques. 28
2.2 Comparison between different encryption methods. 32
2.3 Different between Chaotic Cryptosystem and Traditional Cryptosystem. . . . 42
2.4 Relationship between Chaos Theory and Cryptography. 42

List of Abbreviations

5G	5^{th} Generation
AES	Advanced Encryption Standard
AMF	Access and Mobility Management Function
AODs	Angle of Departures
APD	Avalanche Photodiode
AUSF	Authentication Server Function
BBUs	Baseband Units
BER	Bit Error Rate
C-RAN	Cloud Radio Access Network
CFI	The Choquet Fuzzy Integral
CLM	Channel Load Measurement
CW	Continuous Wave
DES	Data Encryption Standard
EAM	Electro-Absorption Modulator
ECC	Elliptic Curve Cryptography
EDFA	Erbium-Doped Fiber Amplifier
FSO	Free Space Optic
Gbps	Gigabits per second
HAPs	High Altitude Platforms
IM/DD	Intensity Modulation / Direct Detection
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISI	Inter-Symbol Interference
ISM	Industrial, Scientific and Medical
IWT	Integer Wavelet Transform
LD	Laser Diode
LDPC	Low-Density Parity-Check

LED	Light Emitting Diode
LOS	Line of Sight
MATLAB	MATrix LABoratory
MIMO	Multiple Input Multiple Output
MSE	Mean Squared Error
MZM	Mach–Zehnder Modulator
NaaS	Network as a Service
NG-RAN	Next Generation Radio Access Network
NRZ	Non-Return to Zero (line coding scheme)
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDU	Protocol Data Unit
PIN	Positive-Intrinsic-Negative
PLS	Physical Layer Security
PRNGs	Pseudo-Random Number Generators
QoS	Quality of Service
QKD	Quantum Key Distribution
RC4	Rivest Cipher 4
RF	Radio Frequency
RRHs	Remote Radio Heads
RSA	Rivest–Shamir–Adleman
SANs	Storage Area Networks
SKA	Square Kilometre Array
SMF	Session Management Function
SNR	Signal-to-Noise Ratio
SOA	Semiconductor Optical Amplifier
SSIM	Structural Similarity Index Measure
UE	User Equipment
UDM	Unified Data Management
UAVs	Unmanned Aerial Vehicles
UPF	User Plane Function
WinRAR	Windows Roshal ARchive
WinZip	Windows Zone Information Protocol
XOR	eXclusive OR
RK4	Runge-Kutta 4^{th} Order (method)

General introduction

The rapid evolution of information and communication technologies is accompanied by an increasing demand for high data rates, low latency, and enhanced security. In this context, Free Space Optical (FSO) communication systems are emerging as a promising alternative to traditional wireless technologies. By exploiting the propagation of light beams through the atmosphere, these systems enable very high-speed data transmission without physical infrastructure, while providing natural immunity to electromagnetic interference .

Despite these advantages, FSO systems remain highly sensitive to environmental conditions such as fog, rain, and atmospheric turbulence. These factors can significantly degrade signal quality, limiting transmission range and reliability. Therefore, simultaneously improving the robustness and security of FSO links has become a major scientific and technological challenge, particularly regarding their integration into fifth-generation (5G) wireless networks.

This research aims to design and validate a secure FSO communication architecture based on chaotic encryption techniques. Chaotic dynamical systems offer a lightweight and efficient solution to strengthen physical-layer security. The main objective is to leverage chaotic properties to generate robust encryption keys while ensuring stable transmission performance under various atmospheric conditions.

This dissertation is structured into three main chapters:

- The first chapter introduces the fundamental concepts of FSO systems and their potential integration into 5G networks. It outlines their advantages, key components, and major technological limitations.

- The second chapter focuses on security considerations, reviewing various cryptographic approaches and highlighting the effectiveness of chaos-based techniques, particularly through the use of the Chua circuit.

- The third chapter presents the modeling, simulation, and performance evaluation of the proposed system using MATLAB and OptiSystem platforms. Experimental results

are analyzed based on key indicators related to both resistance and robustness. Metrics such as MSE, key space, and entropy are used to evaluate the system's resistance to cryptographic attacks, while indicators such as the Lyapunov exponent, Bit Error Rate (BER), Q-factor, and overall resilience under adverse atmospheric conditions reflect the system's robustness and performance stability.

This work aims to contribute to the state of the art in secure optical communications by demonstrating the relevance of chaos-based methods in meeting the increasing performance and confidentiality requirements of next-generation communication networks.

Chapter 1

Fundamentals of 5G Networks and FSO communications

1.1 Introduction

Mobile communications have undergone a significant evolution, progressing from basic voice calls and text messaging to sophisticated, high speed -data transmission that has radically changed human interaction over the years. The exponential increase in subscription numbers and data consumption has resulted in an unprecedented growth data traffic. Hence, there arose an urgent need to upgrade the existing infrastructure and communication technologies in order to satisfy the Quality of Service (QoS) demands from multiple data streams [1]. In an effort to cope with these challenges, standardization organizations and telecommunication research institutes are in continuous development of protocols and technologies to support high-speed data exchange in the future Fifth-generation (5G) mobile networks represent one of the most promising advancements in wireless communication. 5G backhauls promise a higher bit rate, more reliable services, and seamless connection of billions of devices into the core network. The ultimate aim of next-generation 5G networks is the enhancement of performance metrics such as channel capacity, power efficiency, integration flexibility, and throughput. However, enabling efficient and fast communication remains challenging especially in areas where conventional wired or wireless infrastructure is unavailable or impractical [2]. The integration of Free-Space Optical (FSO) communications within the core of 5G networks proves to be a potential remedy to this anomaly. Free-Space Optics provides communication between base stations, backhaul links, and end-users without the need for physical infrastructure; thus, enabling high-speed, high-bandwidth communications

[3]. This chapter presents an overview of 5G networks and Free-Space Optical (FSO) communication, highlighting their key features, applications, and challenges. It also explores the principal functions, advantages, and limitations of FSO systems and their use in wireless communication. Additionally, it addresses the challenges faced by 5G, particularly to backhaul connectivity, and explains how the implementation of FSO technology can be leveraged to enhance network performance, delivering high-speed, low-latency, and cost-effective communication solutions.

1.2 Free Space Optic (FSO) communications systems

1.2.1 Definition

FSO (Free Space Optics) is a line-of-sight communication with a method that provides high-speed optical bandwidth connections using light traveling in free space, i.e., air or vacuum. It is widely used in computer networks and telecommunications. FSO communication has been in use for several years, and there is increasing demand for secure, tap-free communication and high data rate transfer. FSO is especially well-adapted for satellite communications, deep-space missions, ground stations, Unmanned Aerial Vehicles (UAVs), High Altitude Platforms (HAPs), aircraft, and comparable networks. Because of its spectrum efficiency, bandwidth, and security benefits, FSO is becoming an important complement to RF communications, the next generation of network-centric connectivity [4].

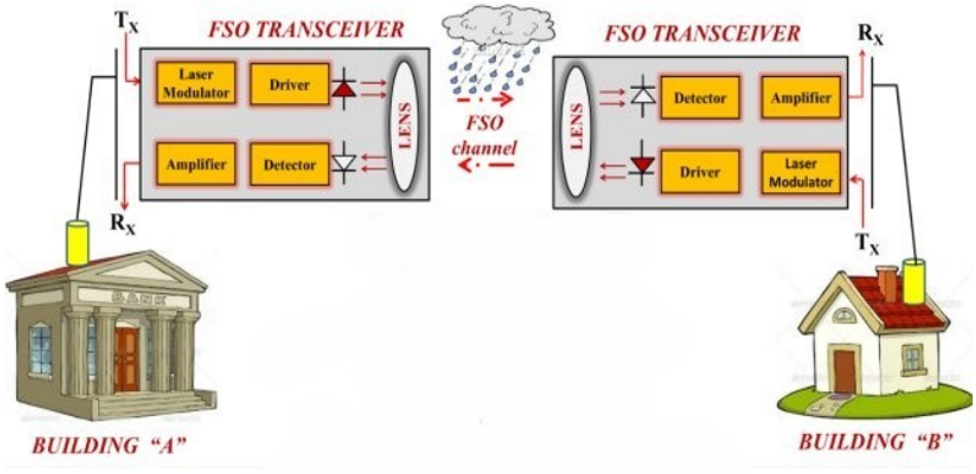


Figure 1.1: The FSO System [5].

1.2.2 Key Features

The FSO system has many key features [6]:

- **High-Bandwidth Availability:** FSO systems operate in the optical domain, utilizing carrier frequencies in the range of hundreds of terahertz, which theoretically enables extremely high channel capacities.
- **Narrow Beam Width:** Since FSO uses a laser at the transmitter end, the beam width is extremely narrow enabling a high level of security that is difficult to achieve with RF communication.
- **Unlicensed Spectrum:** FSO systems operate in the infrared spectrum, which is generally unlicensed (e.g., the ISM band). So, Therefore, FSO is not subject to spectrum allocation regulations, making it cost-effective and easy to deploy.
- **Low Installation Cost:** The installation cost of FSO systems is significantly lower than that of RF for achieving the same data rate.

1.2.3 Applications

The primary applications of FSO systems are outlined below [7]:

- **Storage Area Networks (SANs):** FSO can be integrated with SAN configurations to facilitate data storage, retrieval and inventory management for both integrated and standalone data repositories.
- **Remote Outdoor Communication:** FSO enables unlicensed permission-free communication, making it an ideal solution for organizations operating in remote or hard-to-reach locations.
- **Fiber optic reinforcement:** Serves as a backup for fiber-optic networks, ensuring uninterrupted communication in the event of fiber failure.
- **Cell Network Improvement:** Provides high-speed data delivery for cell mobile networks, enhancing performance and connectivity.
- **Military Applications:** Provides a secure, rapid, and difficult-to-intercept communication network suitable for a range of military uses, including satellite communication, ship-to-shore links, unmanned aerial vehicles (UAVs), drones, and ground-based operations.

- **5G Backhaul and Beyond:** With the ongoing expansion of 5G infrastructure, the demand for high-capacity backhaul solutions is increasing. FSO technology offers gigabit-level data rates and low latency, serving as an effective alternative in environments where fiber deployment is impractical. It enables seamless interconnection between network nodes [8].



Figure 1.2: Free Space Optics (FSO) links are employed to enable 5G connectivity within smart city networks [9].

1.2.4 Components of FSO Systems



Figure 1.3: FSO Communication .

Free-space optical FSO systems are essential to modern telecommunications, enabling line-of-sight (LoS) data transmission through the atmosphere and space. As shown in Figure 1.3, an FSO system consists of three main components: the transmitter (Tx-source), the propagation channel, and the receiver (Rx-destination). Each of these components plays a crucial role in ensuring the efficient transmission of optical signals across free space [10].

1.2.4.1 Transmitter side

The FSO transmitter (Tx) converts electrical data into optical signals using a laser diode (LD) or LED. It incorporates beam-forming to ensure precise signal direction, Optional components such as modulators, amplifiers, and channel coding units may be included to improve transmission efficiency. A typical Tx system consists of an optical source, a modulator, an amplifier (if required), and optical elements designed to maintain reliable data transmission across free space [10].

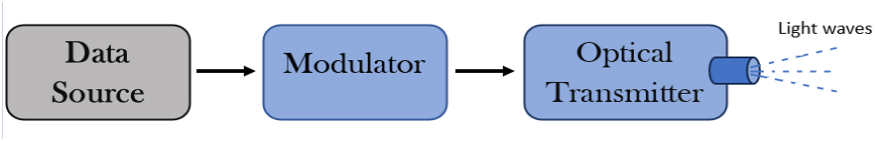


Figure 1.4: block diagram of Transmitter side in FSO system.

Optical sources: Optical sources are active elements that turn electric energy into optical energy. The growing call for greater bandwidth requires the effective optical source availability. Usually these sources are [11]:

- **Light-Emitting Diodes (LEDs):** LEDs are incoherent, polychromatic light sources characterized by a relatively broad emission spectrum and a less directional radiation pattern Thay are typically used in optical transmission systems that do not require high bandwidth.

  - Optical power output: up to several hundred micro watts.
  - Data rate: typically, less than 5 Mbit/s when used with multimode fiber.

- **Laser Diodes (LDs):** Laser diodes are semiconductor optoelectronic components that operate based on three fundamental physical mechanisms: absorbance, spontaneous emission, stimulated emission. These mechanisms allow the generation and amplification of coherent light within the diode structure. Laser diodes are widely used in Free-Space Optical (FSO) communication systems due to several advantages:

  - They operate at higher frequencies, enabling increased modulation rates.
  - They emit a highly directional beam, allowing efficient long-distance transmission with minimal dispersion.

- Optical transmitters must meet several key requirements, including:
  - Stable operation at room temperature.
  - Capability to modulate the emitted light at high frequencies.
  - High Optical output power.
  - Long operational life time.

Signal Modulation: In optical communication systems, modulation is a fundamental mechanism for transmitting information. Two main approaches are commonly used: direct modulation and external modulation. These methods enable the rapid encoding of data onto an optical carrier signal [11]:

- **Direct modulation:** is a simple and cost-effective technique in which the laser's driving current is directly varied according to the digital input signal. This variation modulates the optical output power. However, this approach becomes inefficient at data rates above 2.5 Gb/s due to signal degradation. Specifically, modulating the current alters the refractive index of the laser cavity, resulting in unwanted frequency chirping—a major limitation for high-speed transmissions.

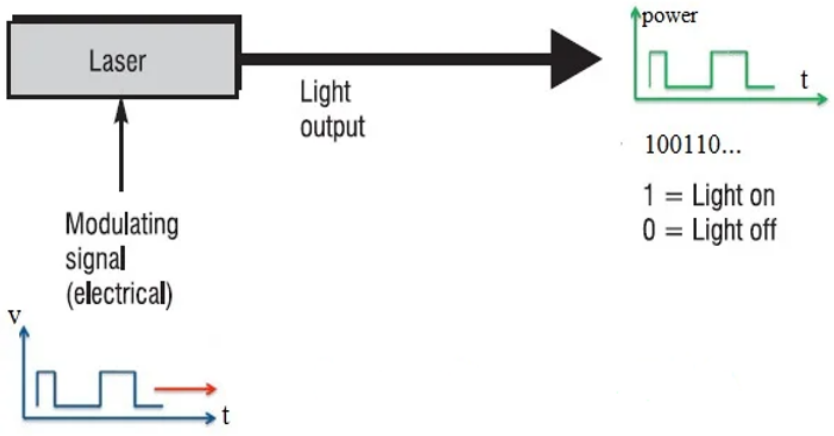


Figure 1.5: Laser diodes are modulated directly by varying the injection current.

- **External modulation:** is achieved by modulating the optical signal after it exits the laser diode, which operates in continuous-wave (CW) mode. This differs from direct modulation, where the driving current of the laser is varied. As a result, external modulation significantly reduces the chirp effect, thereby minimizing its impact on the transmitted optical signal.

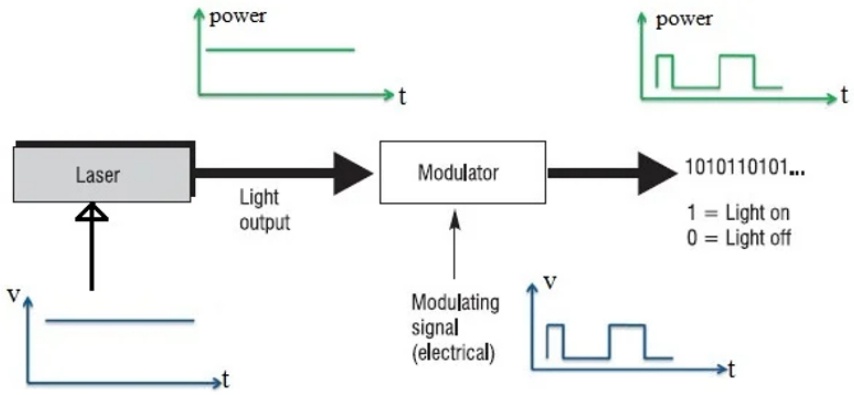


Figure 1.6: Laser diode using external modulation.

Several types of modulators are employed in optical communication Systems. Among the most commonly used are the Mach-Zehnder modulator (MZM) and the electro-absorption modulator (EAM), both of which play critical roles in high-speed optical signal modulation [11]:

- **Mach-Zehnder Modulator (MZM):** As illustrated in Figure 1.7, a Mach-Zehnder Modulator (MZM) operates by splitting an incoming optical signal into two distinct optical paths. When a voltage is applied to one of these paths, it induces a change in the refractive index, resulting in a phase shift of the optical wave. The two paths are then recombined after propagating over a certain distance, forming an interferometric structure. This configuration—commonly referred to as an interferometer—produces interference between the two signals. The nature of this interference, whether constructive or destructive, depends on the relative phase difference between the paths, ultimately determining the amplitude of the output optical signal[11].

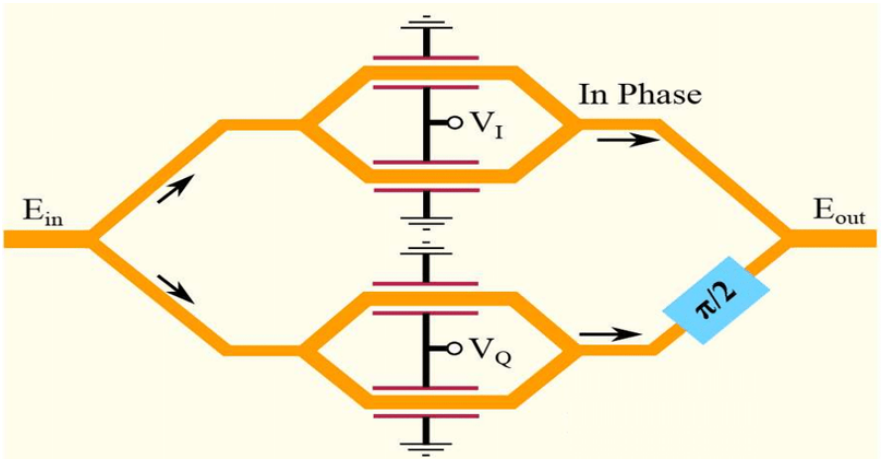


Figure 1.7: Operating Principle of the Integrated Mach-Zehnder Modulator.

- **Electro-Absorption Modulation (EAMs):** Electro-absorption modulators operate by modifying the intensity of an optical signal through a material whose absorption properties change under the influence of an electric field. A key advantage of EAMs is their compact size, making them well-suited for deployment in urban optical networks. Additionally, they can be seamlessly integrated with continuous-wave laser diodes. However, EAMs typically exhibit higher insertion losses—often at least 10 dB—compared to Mach-Zehnder modulators (MZMs).

Amplificatory: Optical amplification compensates for transmission losses without requiring costly electronic regenerators. This process is based on stimulated emission, where an external energy source referred to as pumping, is used to amplify the optical signal [11], There are two types of Amplificatory:

- **Semiconductor Optical Amplifiers (SOAs):** are devices that provide optical gain through an electrically pumped active region. Depending on their placement within the optical link, they can serve as booster amplifiers, inline amplifiers, or preamplifiers.

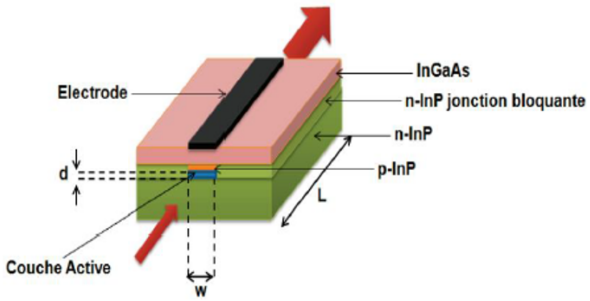


Figure 1.8: Semiconductor Optical Amplifiers (SOAs).

- **Erbium-Doped Fiber Amplifiers (EDFAs):** are crucial components in optical in telecommunications, enabling the simultaneous amplification of multiple wavelengths. These amplifiers utilize optical fibers doped with Er3 + ions, which are optically pumped - typically by laser diodes - to achieve population inversion. This condition facilitates signal amplification via the mechanism of stimulated emission.

1.2.4.2 Receiver side

In a Free-Space Optical (FSO) communication system, the receiver (Rx) captures the transmitted optical signal and converts it into an electrical signal. It typically comprises a photodetector—such as a PIN diode or an avalanche photodiode (APD)—which converts the incoming light into an electrical current. APDs are generally preferred due to their high sensitivity, enabling the detection of weak optical signals over long distances [10].

Following photodetection, a transimpedance amplifier converts the weak current into a voltage signal. This signal is subsequently amplified to enhance clarity. Demodulation is then performed, along with signal combination if spatial or temporal multiplexing was used during transmission. Noise is reduced through filtering, and a Low-Density Parity-Check (LDPC) decoder is applied to correct errors and recover the original transmitted data with high accuracy [8].

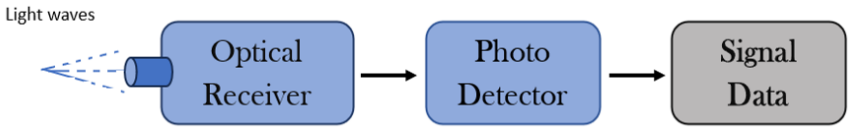


Figure 1.9: Block diagram of the Receiver side in FSO systems.

Photodetectors: Photodetectors are electronic components that convert optical pulses, typically received through optical fibers into electrical signals. Depending on application-specific requirements, different types of photodetectors can be employed. The most commonly used are [12]:

- **Positive Intrinsic Negative (PIN) Photodiode:** is a type of p-n junction diode that incorporates an intrinsic (undoped) layer between the p- and n-type regions. When reverse biased, increasing the bias voltage expands the depletion region, thereby enhancing the generation of photocurrent in response to incident light.

- **Avalanche Photodiode (APD):**Structurally similar to the PIN photodiode, the APD operates under a significantly higher reverse bias voltage. This elevated bias facilitates impact ionization, a process that amplifies the photocurrent by generating additional charge carriers, thus improving the device's sensitivity and enabling internal gain.

1.2.4.3 Propagation Channel

In FSO communication system, the propagation channel refers to the atmospheric or free-space or medium through which optical signals travel. Unlike fiber optic systems that utilize physical cables. This reliance on line-of-sight (LoS) renders the channel particularly susceptible to environmental disturbances such as atmospheric turbulence, weather conditions, and physical obstructions[10].



Figure 1.10: Propagation Channel in FSO system.

The atmospheric medium, a complex and dynamic component of the propagation channel, can specifically influence the characteristics of the radiated laser beam. Environmental factors particularly atmospheric phenomena, such as Precipitation (e.g., rain and snow), can induce attenuation or extinction of the optical signal in during propagation, thereby limiting the effective range between the transmitter and the receiver, as illustrated in Figure 1.11[13].

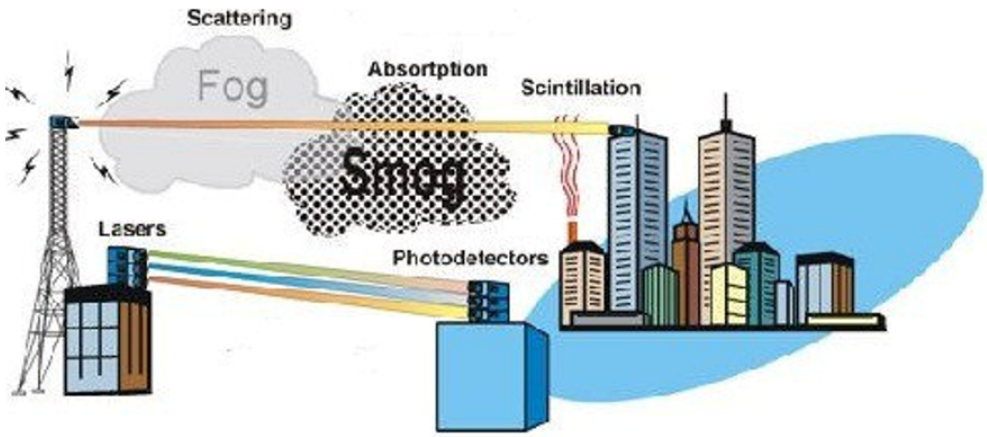


Figure 1.11: Atmospheric medium between the transmitter and receiver in FSO communication systems.

1.2.5 Challenges

Free-space optical technology offers extremely high data rates and low latency. However, its performance is significantly influenced by on environmental conditions. One of the most critical challenges in free-space optical systems is signal degradation caused by atmospheric conditions, which results in increased attenuation and reduced transmission reliability.

- **Atmospheric attenuation:** As electromagnetic wave energy propagates through the atmosphere it experiences c attenuation -defined as the gradual loss of signal power y. This phenomenon occurs due to absorption and scattering by atmospheric constituents such as gases, aerosols, dust, and other suspended particles. The attenuation process is commonly modeled using Beer's Law[11], which states:

$$I = I_0 e^{(-\beta.L)} \tag{1.1}$$

Where:

- I_0: The initial light intensity at the source.

- I: The remaining light intensity after traveling a distance L.

- β: The total attenuation coefficient.

- L: The propagation distance through the medium.

The attenuation factor (Att) represents the ratio of the output intensity to the input intensity, i.e., how much of the original signal remains:

$$Att = e^{(-\beta.L)} \tag{1.2}$$

Where:

- Att: Atmospheric attenuation.
- β: Total attenuation coefficient, given by $\beta = \beta_{abs} + \beta_{scatter}$.
- β_{abs}: Molecular absorption coefficient of the aerosol.
- $\beta_{scatter}$: Molecular scattering coefficient of the aerosol.

Foggy atmosphere

Accurately measuring fog density and extracting reliable statistical data are challenging tasks, primarily because these parameters are typically derived from airborne particulate concentrations. The reduction in signal strength due to fog, expressed in decibels per kilometer (dB/km), is inversely proportional to atmospheric visibility (V) measured in kilometers (km). Studies have shown that the attenuation coefficient ($\in$) typically ranges between 0.02 and 0.05, and it can be expressed by the following equation:

$$Att_{fog} = |10\log_{10}(\in)/V| \tag{1.3}$$

Where:

- $\in$: Atmospheric transmission coefficient represents the fraction of optical signal power that is transmitted through the atmosphere without being absorbed or scattered (values range between 0 and 1, where 1 = full transmission and 0 = total attenuation).
- V: Visibility range – the maximum distance (in Km) at which an object can be clearly seen in foggy or hazy conditions; lower values indicate denser fog and higher signal attenuation.

Rainy Atmosphere

Rain-induced attenuation of radio signal primarily results from geometric scattering, a phenomenon occurring when the signal interacts with raindrops. This scattering affects signal propagation and requires careful consideration. Raindrops act as agents of reflection and refraction for electromagnetic waves, leading to a degradation of signal integrity. The

attenuation caused by precipitation, typically measured in decibels per kilometer (dB/km), can be modeled using the following equation:

$$Att_{rain} = 1,076 * R^{0.67} \tag{1.4}$$

Where:

- Att_{rain}: Rain attenuation represents the signal loss (in dB/km) caused by rain along the transmission path.
- R: Rainfall rate the intensity of rain in millimeters per hour (mm/h); higher rainfall leads to greater attenuation.
- 1.076: Empirical constant – a coefficient derived from experimental data to fit the model to real-world measurements of attenuation due to rain.

Scintillation

When solar radiation heats the earth's surface, the adjoining layers also warm up but not uniformly. As a result, localized air pockets with different temperatures form, leading to spatial variations in the refractive index of the atmosphere. These fluctuations affect the propagation path of optical signals, causing random intensity variations, commonly referred to as scintillation. This phenomenon results in signal power loss, thereby degrading the performance and availability of free-space optical communication links [14].

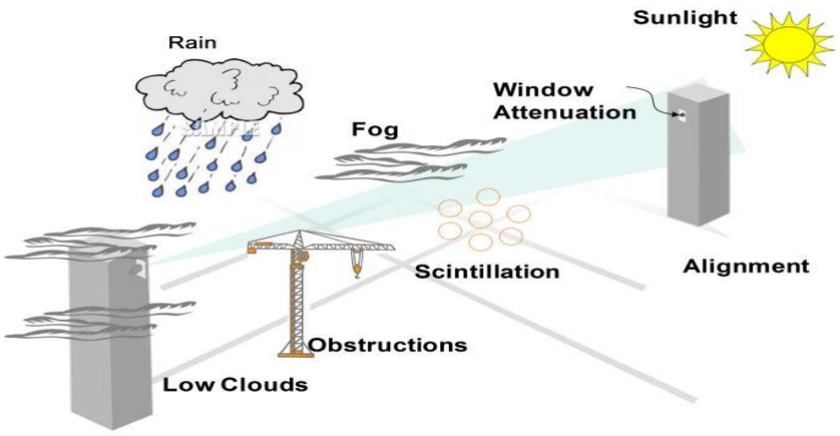


Figure 1.12: Effects of various physical and weather conditions on the FSO.

- **Loss in Beam Degrees:** Diffraction causes the optical beam to to expand as it propagates through the atmosphere This expansion may result in beam divergence loss if the receiver's aperture is insufficient to capture the entire transmitted beam.

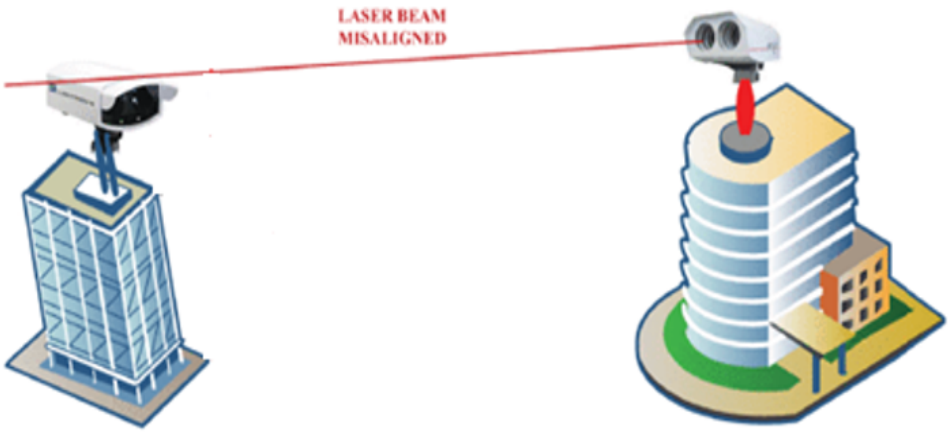


Figure 1.13: Laser beam misalignment between FSO transceivers [5].

1.2.6 Comparison with Fiber Optic and Free Space Optical Communication

Free Space Optics (FSO) and fiber-optic transmission share similar underlying principles, however, FSO employs air as the transmission medium rather than optical fiber. Although fiber optics is known for its high reliability, its deployment remains costly and lacks flexibility. In contrast, FSO offers a cost-effective solution for short-range communication (typically between 200 and 2000 meters), delivering high bandwidth and effectively addressing the 'last mile' connectivity challenge [15].

Table 1.1: Comparison between FSO and fiber optic

Feature	**Free Space Optics (FSO)**	**Fiber Optics**
Deployment Time	Ranges from a few days to several weeks	May take several months to years due to civil works
Provisioning Time	Almost Immediate	Longer, requires trenching and physical cable installation
Initial Investment	Low to moderate	High, due to infrastructure and material costs

Feature	Free Space Optics (FSO)	Fiber Optics
Reliability	Moderate to low; significantly affected by atmospheric conditions	Very high; stable under most environmental conditions
Distance Limitation	Up to 2 km (optimal conditions)	Up to 100s of km (with repeaters)
Bandwidth/Speed	Up to 10 Gbps under ideal conditions	Up to Tbps with advanced fiber networks

1.3 5G Networks

1.3.1 Definition

5G technology represents a significant evolution in wireless communications, offering substantial improvements in speed, latency, and connectivity. It enables both consumers and enterprises to connect a wide range of devices, enhancing user experience, network performance, and reliability. Furthermore, 5G facilitates the deployment of new services and applications, contributing to the realization of the "Internet of Everything." This technology supports a broad spectrum of sectors, including healthcare, automotive, education, manufacturing, and agriculture, particularly in meeting their service-oriented (or "soft") needs. By integrating virtualization and softwarization, 5G networks can accommodate multiple types of PDU (Protocol Data Unit) sessions—such as IPv4, IPv6, Ethernet, and unstructured PDUs. Additionally, through dynamic network slicing, 5G enables the concept of "Network as a Service" (NaaS), optimizing multi-operator scenarios to ensure enhanced efficiency, scalability, and flexibility [16].

1.3.2 Key Features

The fifth-generation mobile network, commonly referred to as 5G, represents a major advancement in mobile communication technologies. Its ultra-high-speed capabilities have the potential to revolutionize the use of mobile devices, enabling smartphones to perform at levels comparable to laptops thanks to enhanced technical functionalities.
The main features of 5G are summarized in table the bellow [17]:

Table 1.2: Key Features of 5G

Features	**Description**
Speed	Up to 10 Gbps
Latency	As low as 1 ms
Spectral efficiency	Five to fifteen times higher than 4G
Energy Efficiency	improved by more then 100 times
Internet speed	Fast and highly reliable
Frequency Band	Ranges From 1 GHZ to 24 GHZ
Access technique	Orthogonal Frequency Division Multiplexing (OFDM)

1.3.3 Applications

- **Disaster Recovery and Emergency Response:** FSO-5G networks can be rapidly deployed to restore connectivity in areas where infrastructure has been damaged or destroyed by natural disasters. The ease of deployment and high adaptability of FSO systems make them particularly well-suited for emergency response scenarios, ensuring reliable communication when it is most critical [18].

- **Combining with Aerial Platforms:** An emerging approach to extending 5G network coverage involves the deployment of unmanned aerial vehicles (UAVs) equipped with free-space optical (FSO) transceivers. These aerial base stations provide on-demand network access, enhancing connectivity and performance in both urban and remote areas [14].

- **Autonomous Driving Technology:** The deployment of 5G technology is accelerating the development of autonomous driving, bringing it closer to practical realization. However, key challenges must first be addressed to ensure improved overall traffic safety. Intelligent material technologies enable vehicles to perceive roads similarly to human drivers, which is a critical capability for the advancement of future smart cities [19].

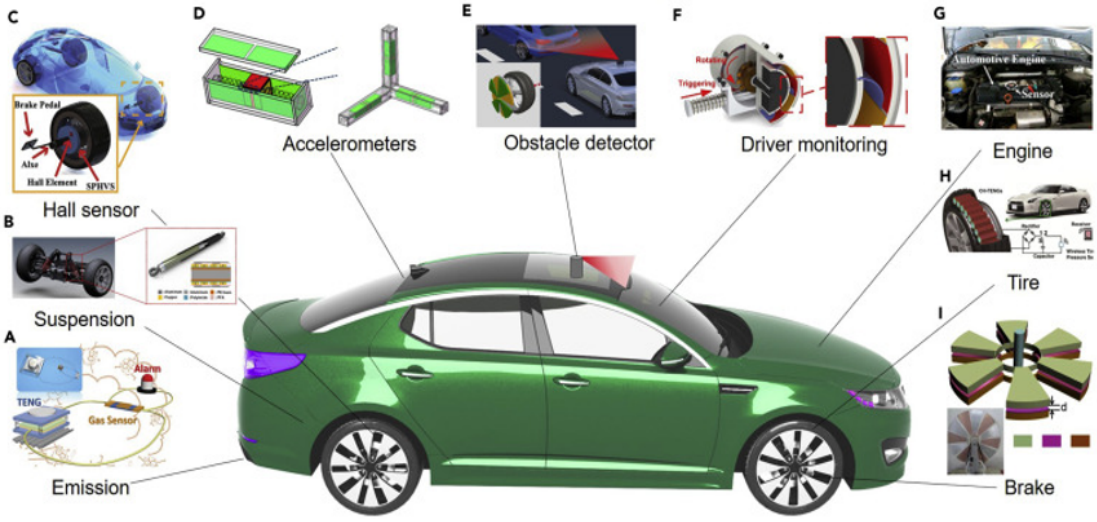


Figure 1.14: Autonomous-driving in the Context of 5G Networks.

- **Human-machine interaction:** With the deployment of 5G in urban environments, human-machine interaction is experiencing significant growth. This trend necessitates enhanced levels of security, privacy, reliability, and user convenience, particularly for connected devices such as fitness bands, smartphones, and tablets. As illustrated in Figure 1.14, devices that incorporate human-machine interfaces can be categorized into four main types: text-based user interfaces, touch-based interfaces, voice-controlled interfaces, and body motion tracking interfaces.

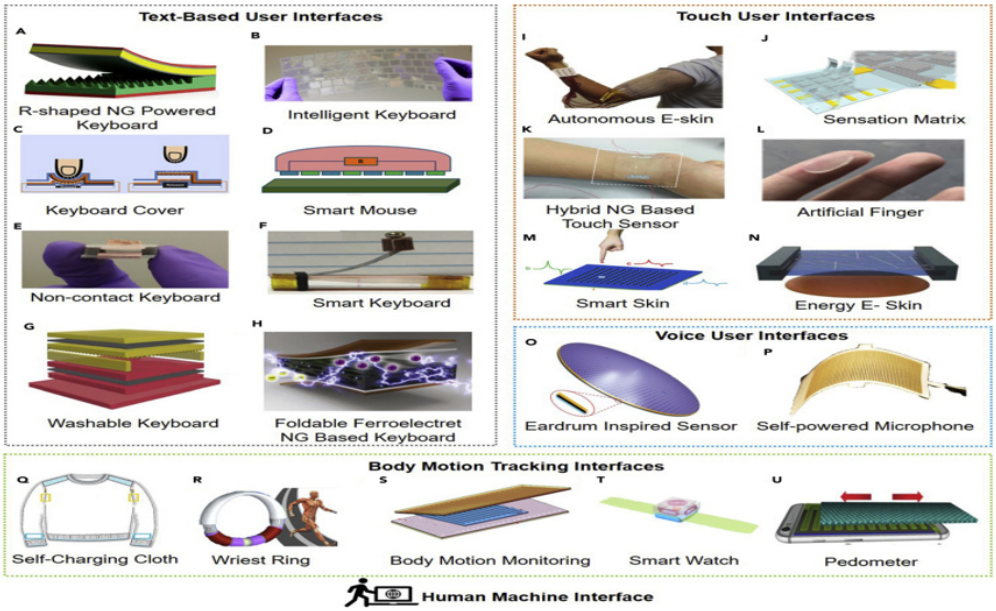


Figure 1.15: Human-machine interface in 5G environments.

- **Smart Healthcare:** The primary objective of smart healthcare is to improve the accuracy of digital health monitoring systems and to enhance diagnostic and therapeutic processes by integrating advanced technologies with medical expertise. This integration enables more efficient and personalized healthcare services, as depicted in Figure 1.16.

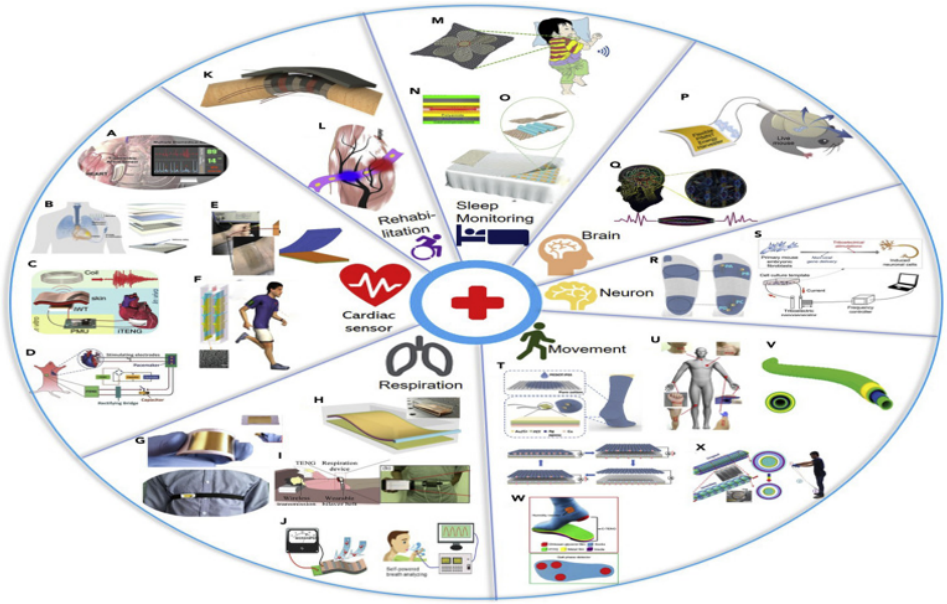


Figure 1.16: Smart healthcare in the context of 5G.

1.3.4 Challenges

5G technology offers a promising a solution for the growing demand for high-speed, high-capacity communication networks, However, several challenges must be addressed to ensure cost-effectiveness and optimal performance. These include:

- **High Operational Costs:**The deployment and maintenance of 5G networks entail significant operational expenses due to the need for increased capacity, advanced infrastructure, and energy-intensive equipment. Although 5G reduces the energy consumption per transmitted bit, the overall operational energy remains substantial [20].

- **Security and Privacy:**Wireless networks inherently face more security vulnerabilities than wired systems, including risks of unauthorized access, cyberattacks, and data interception. Additionally, the large bandwidth and high-power consumption of 5G increase these risks. Ensuring data privacy is therefore a critical concern in the design and implementation of 5G systems [20].

- **Low Latency:**Achieving ultra-low latency, a core requirement of 5G, poses considerable technical challenges. Key bottlenecks lie in the radio access network (RAN), core network architecture, backhaul connectivity, edge caching mechanisms, and overall resource management strategies [21].

- **High Capacity:**Meeting high-capacity demands is constrained by spectrum scarcity, the significant propagation losses associated with millimeter wave (mmWave) frequencies, and the necessity of deploying dense small-cell networks to maintain signal quality and coverage [22].

1.3.5 Architecture

The 5G system is composed of a 5G Radio Access Network (i.e., NG-RAN: Next Generation RAN) and a 5G Core Network, as illustrated in figures bellow [23]:

- **Radio Access Network:**The 5G Radio Access Network is made up of base stations (gNBs) that connect mobile devices to the 5G core. Devices can connect via a 5G link (gNB) or an enhanced 4G link (ng-eNB). Unlike the traditional eNB used in 4G systems, the gNB manages Quality of Service (QoS) on a per-flow basis and supports network slicing, enabling the optimization of services according to specific user or application requirements.

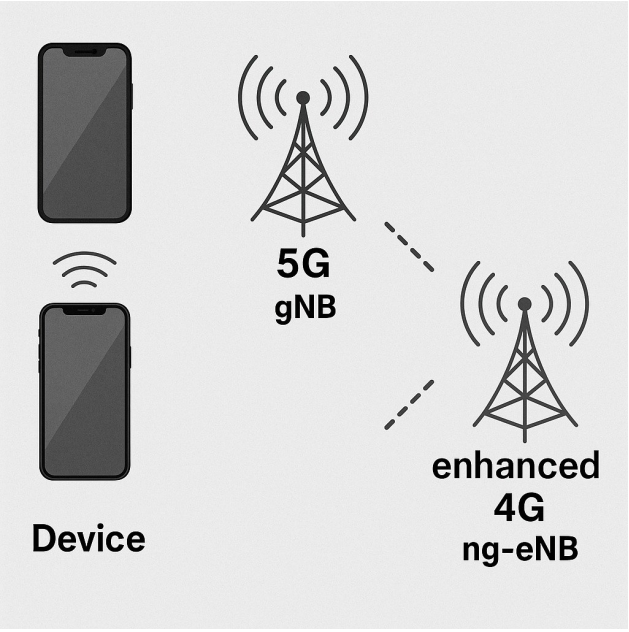


Figure 1.17: 5G RAN Network.

- **Core Network:** The 5G core network is based on a service-based architecture and consists of several essential functional components. The Access and Mobility Management Function (AMF) is responsible for managing access and mobility. The Session Management Function (SMF) oversees session management, while the User Plane Function (UPF) handles data transfer between user equipment (UE) and the external data network.

For authentication and security, the Authentication Server Function (AUSF) provides authentication services, and the Unified Data Management (UDM) serves as a centralized repository for user data. The Policy Control Function (PCF) is tasked with enforcing policy and traffic management rules. In addition, the Network Slice Selection Function (NSSF) facilitates the selection of appropriate network slices. All these components interact through standardized service-based interfaces, forming the backbone of the 5G core network.

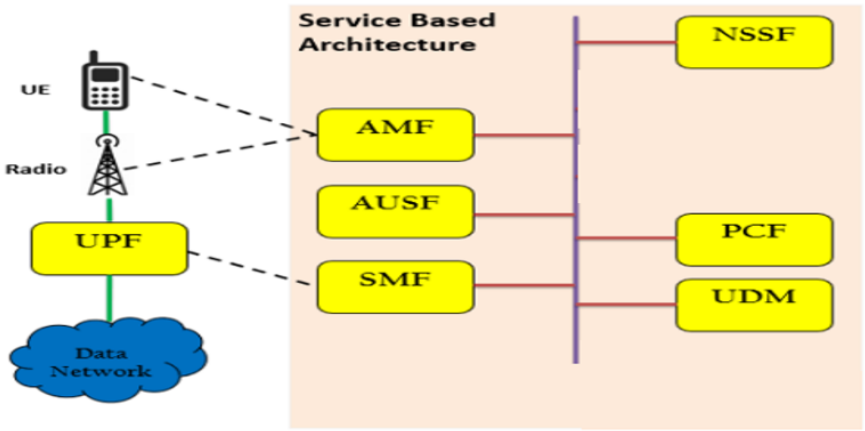


Figure 1.18: 5G Core Network.

Although 5G networks are addressing increasing user demands, traditional architectures struggle to accommodate the rising traffic and connectivity requirements. One of the most significant innovations in 5G is the adoption of Centralized Radio Access Networks (C-RAN), in which Baseband Units (BBUs) are decoupled from Remote Radio Heads (RRHs). This architectural shift necessitates the deployment of cost-effective fronthaul and backhaul technologies [22].

- **Fronthaul** refers to the link between RRHs and centralized BBUs.
- **Backhaul** connects the access network to the core network, handling vast volumes of traffic while requiring high bandwidth and low latency.

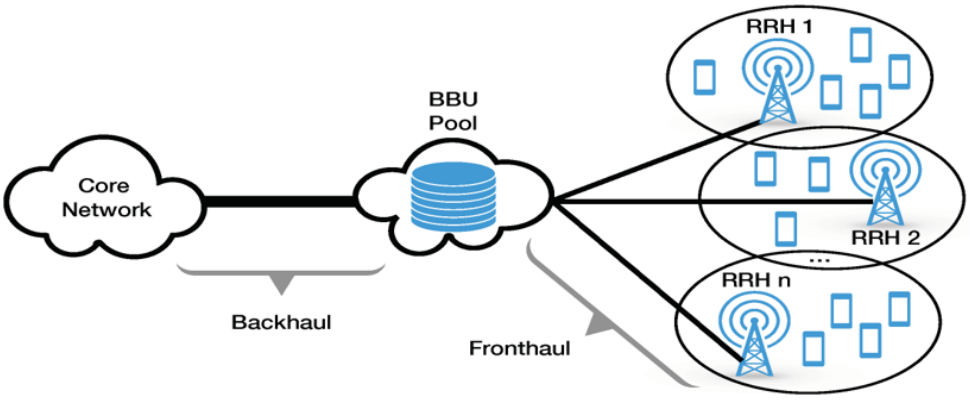


Figure 1.19: 5G Architecture Backhaul /Fronthaul [22].

Various technologies have been proposed for 5G fronthaul and backhaul, each offering distinct advantages and limitations. The main challenges include :

- **High Bandwidth and Capacity Requirements:** 5G networks are expected to handle traffic volumes 100 to 1000 times greater than previous generations, necessitating substantial data transmission capabilities.
- **Low Latency:** Essential for supporting real-time applications such as autonomous driving and remote surgery.
- **Ultra-Dense Connectivity:** Enables the deployment of a large number of small cells, particularly in densely populated urban areas.
- **Deployment Constraints:** In regions where fiber deployment is impractical due to geographic or infrastructural limitations, wireless alternatives such as Free-Space Optics (FSO) present a feasible solution.
- **Long-Distance Connectivity:** The centralized architecture of 5G networks requires reliable long-range transmission links.

1.4 Integration FSO communication in 5G networks

Free-Space Optics (FSO) has emerged as a promising candidate for enhancing 5G networks, offering high bandwidth, low latency, and cost-effective wireless communication. It utilizes light as a carrier in unguided media, presenting several advantages [24]:

- **Easy and Cost-Effective Deployment:** FSO systems do not require physical fiber or cabling, facilitating rapid and economical installation.
- **High Bandwidth and Low Latency:** Capable of supporting data rates up to 2 Gbps, making it suitable for high-speed applications.
- **Long-Range Communication:** Operates effectively over distances ranging from 100 meters to several kilometers.
- **Unlicensed Spectrum Utilization:** Functions in the optical spectrum above 300 GHz (typically 785–1550 nm), free from regulatory licensing constraints.
- **Minimal Electromagnetic Interference:** Naturally immune to radio frequency and electromagnetic interference.

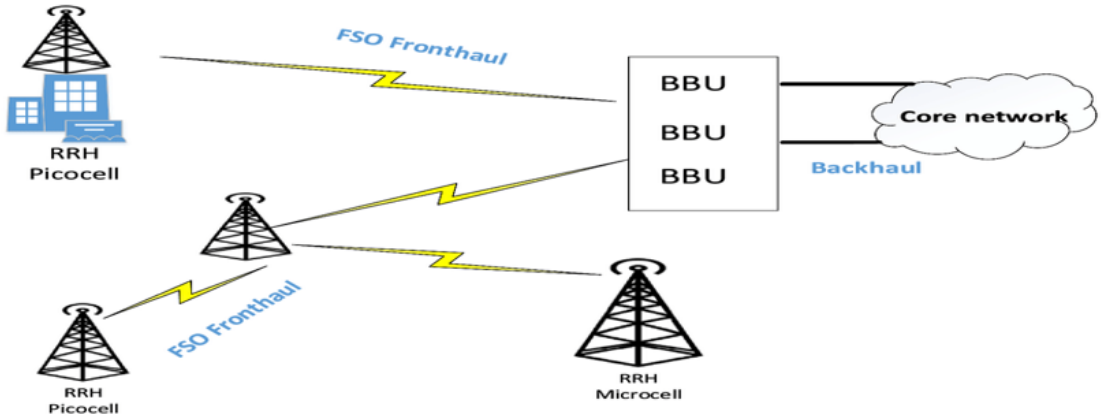


Figure 1.20: Integration of FSO in 5G Architecture [25].

Due to its numerous advantages, Free Space Optics (FSO) is considered an ideal solution for 5G fronthaul and backhaul links. However, FSO systems are significantly affected by atmospheric conditions, which remains one of their main limitations. Ongoing research efforts aim to address and potentially resolve most, if not all, of these challenges.

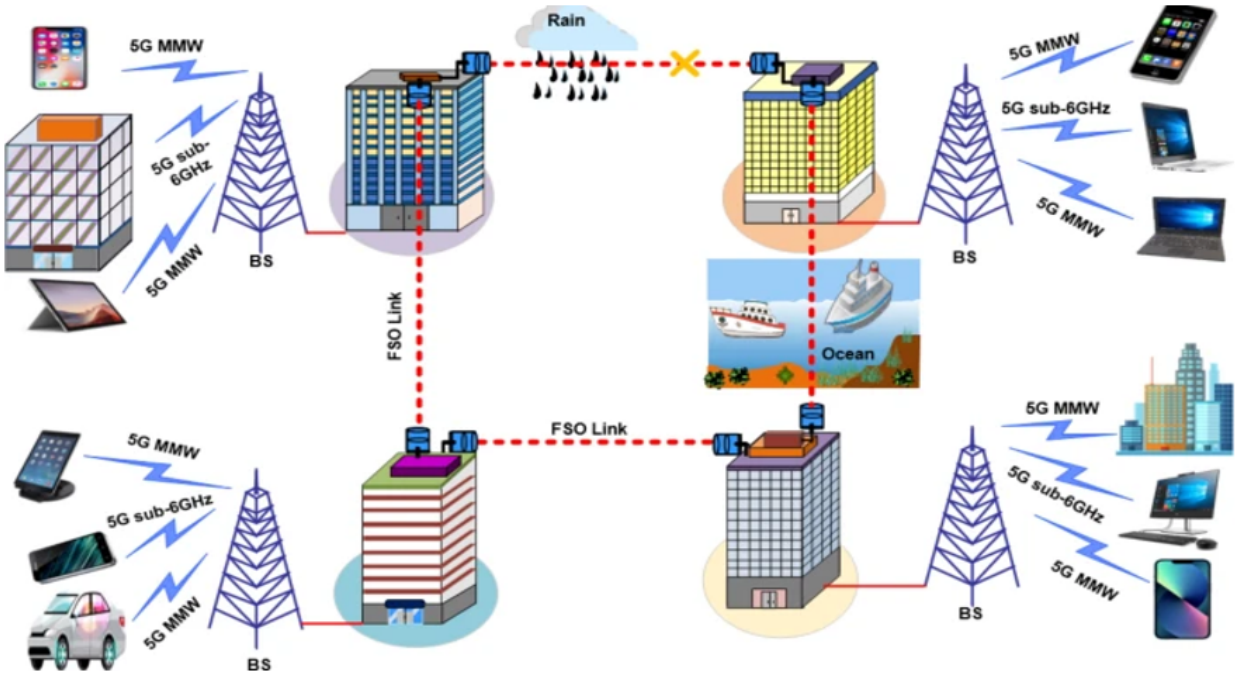


Figure 1.21: FSO link across multiple domains [26].

1.4.1 Conclusion

The integration of Free-Space Optics (FSO) with 5G networks introduces new possibilities for achieving high-capacity, ultra-low-latency backhaul connections, while addressing several limitations associated with conventional 5G deployment. FSO further strengthens network resilience by maintaining connectivity under adverse atmospheric conditions, thereby enhancing the scalability, robustness, and overall performance of next-generation communication infrastructures.

As with traditional 5G networks, which rely on encryption mechanisms to ensure secure data transmission, FSO systems also require strong cryptographic protection—arguably even more so, given the vulnerability of free-space transmission to interception and eavesdropping. Thus, the use of advanced encryption techniques is both necessary and judicious in this context. Chapter 2 delves into a range of cryptographic methods adapted to the specificities of FSO links, addressing critical challenges such as data integrity, confidentiality, and secure key management in high-speed optical communication environments.

Chapter 2

Chaotic approach for securing FSO systems

2.1 Introduction

Free-Space Optical (FSO) communication has has emerged in recent years as a promising solution for secure and high-speed data transmission However, FSO systems are susceptible to external disturbances such as atmospheric turbulence, beam misalignment, and unauthorized interception, which pose significant security challenges. Classical encryption methods, although effective in many scenarios, may fall short of addressing the unique limitations inherent to FSO systems.

To strengthen the security of FSO communications, chaotic encryption methods have been receiving growing interest. These techniques take advantage of the unique characteristics of chaotic systems — such as extreme sensitivity to initial conditions, apparent randomness, and deterministic behavior — to provide robust data protection. Unlike traditional cryptographic methods that mainly depend on computational complexity, chaotic encryption relies on the dynamic behavior of nonlinear systems. Because of this, it is increasingly considered a promising approach for securing optical communication systems [27].

This chapter explores how chaotic systems can be applied to improve the security of free-space optical (FSO) communication. It begins with an overview of general cryptographic techniques, then focuses on encryption methods that are specifically adapted to the unique characteristics of FSO systems. The chapter also introduces mathematical models of chaotic systems — such as the Logistic Map, the Lorenz System, and Chua's Circuit — and explains how these models can be used effectively in encryption. Finally, a comparative analysis high-

lights the strengths and limitations of chaotic encryption in FSO networks, demonstrating its potential to ensure secure and reliable data transmission.

2.2 Encryption Techniques

Cryptography is derived from the ancient Greek words kruptos (hidden) and graphein (to write), meaning "to write in a hidden manner". Cryptography is the science of protecting information from being accessed or interpreted by unauthorized parties. It is the process of encoding readable data into unreadable data using a secret key, referred to as Encryption. The technique of reversing it, called decryption, restores the data to its original, readable form using the same or a related key [28]. Cryptographic security relies on several fundamental principles: confidentiality (protection against unauthorized access), integrity (protection against data modification), authentication (verifying the identity of the sender), and non-repudiation (ensuring the sender cannot deny the transmission). Cryptographic techniques fall into two broad categories [29]:

2.2.1 Symmetric

In secret key or symmetric-key cryptography, the receiver and sender share the same key for both encryption and decryption. We have two types of symmetric ciphers [30]:

- Block ciphers, such as (AES, Blowfish, and Twofish), encrypt fixed-sized data blocks using a shared secret key.
- Stream ciphers such as (ChaCha20 and RC4) encrypt data by combining it with a pseudorandom keystream.
- Encryption strength depends on the complexity of the algorithm and the key size—longer keys and stonger algorithms provide enhance security.

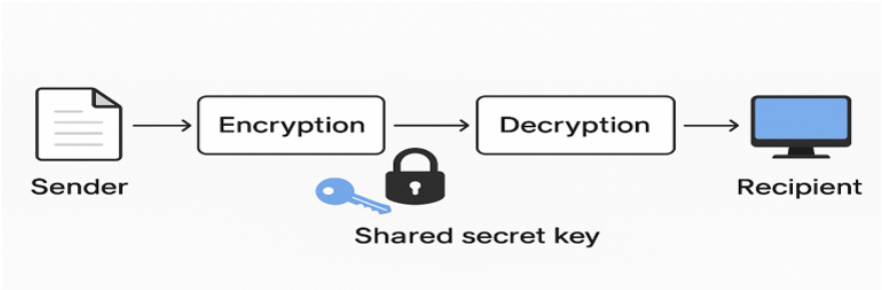


Figure 2.1: Symmetric cryptography.

2.2.2 Asymmetric

In Asymmetric or Public key cryptography, the system uses a pair of keys: a public key for encryption and a private key for decryption. Such schemes are common in algorithms such as RSA and ECC. Public-Key Cryptography enables secure key distribution and supports digital signatures, which authenticate the message and its sender [30].

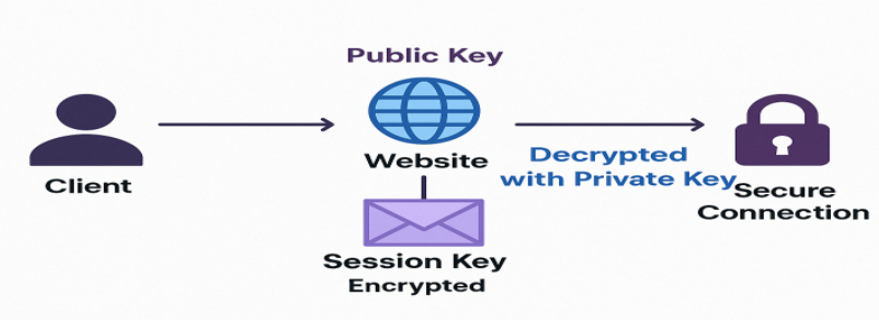


Figure 2.2: Asymmetric cryptography.

Encryption techniques are essential to secure information, and each technique has its own strengths and weaknesses. They differ in terms of speed, security, and key management. This information is used to select the most suitable encryption technique for a given application. The analysis below describes the most critical elements of these techniques [29]:

Table 2.1: Comparison between some encryption techniques.

Comparaison factor	**DES**	**RSA**	**AES**
Designed by	International Business Machines (IBM) in 1970	Rivest, Shamir and Adleman in year 1978	Vincent Rijmen and Joan Daemen 2001
Number of rounds involved	16	Not a round-based algorithm	10, 12, 14
Keys length used	56 bits	Variable	128, 192, or 256 bits
Block length used	64 bits	Variable-length integers	128 bits

Continued on next page

Comparaison factor	**DES**	**RSA**	**AES**
Speed	Slow	Slowest	Fastest
Advantage	Easy to implement	Safe and secure via complex mathematics. Used in financial transactions, business, etc.	Used in a wide variety of applications
Disadvantage	Small key size makes it vulnerable	Very slow in large data encryption	Hard to implement in software
Successors	Triple DES, G-DES, DES-X	No direct successor. Still widely used. ECC is a modern alternative	Anubis, Grand CRU, Kalyna
Structure	Balanced Feistel Network	Based on modular arithmetic and number theory	Substitution-permutation network
Application areas example	Banking sector, ATM PINs	Digital signatures, confidential documents	Encrypting file systems (e.g. WinZip, RAR)

2.3 Adaptation of Encryption techniques to Free Space Optical systems Constraints Related to Optical Performance

Free Space Optical (FSO) communication systems face severe challenges that impact their reliability, primarily caused by environmental factors and system limitations such as atmospheric turbulence and beam misalignment. These problems result in weaker signals, discontinuities, and high errors rates making it difficult to achieve secure and stable communication. To address these challenges many encryption methods have been developed to operate within FSO constraints, as mentioned outlined in the following points:

2.3.1 The Choquet Fuzzy Integral (CFI) and integer wavelet transform (IWT)

As with all free-space optical system, the transmission comes under peril of signal loss while crossing through weather conditions such as rain and fog, clouding their image quality and network reliability. Therefore, in order to syphon off the detrimental effects of poor weather, the techniques of CFI and IWT are employed to bolster security, enhance image quality, and improve system resilience against environmental conditions. The encryption using CFI yields highly secure pseudo-random streams, shielding the data from attacks with a measure of computational efficiency. In contrast, IWT separates the image into sub-bands, which reduces transmission errors and strengthens overall security. Well, perhaps that should all translate towards very tough and secure image transmission under the weather situation [31] [32]:

- In low fog, images are not obscured at longer distances, and CFI encryption filtering improves image quality after decryption.
- In medium-level fog, attenuation reduces the transmission distance, yet CFI encryption strengthens image integrity, and filtering techniques increase SNR and SSIM for improved images.
- During dense fog, transmission is limited by high attenuation, yet CFI encryption ensures data integrity, and image enhancement algorithms optimize visibility.

The integration of CFI encryption, IWT decomposition, and filtering techniques successfully enables the transmission of high-quality images securely in FSO communication under unfavorable weather conditions.

2.3.2 Quantum Key Distribution (QKD)

Quantum Key Distribution offers unconditional security based on the principles of quantum mechanics, making it highly suitable for secure communications. Free-space optical (FSO) channels offer high bandwidth low latency, and support for long-distance data transmission without the need for physical infrastructure. In FSO QKD, information is encoded in quantum states of photons, typically using polarization (linear or circular). The transmitter (Alice) encodes the photons with polarization-based qubits and sends them to the receiver (Bob), who measures them using a compatible basis. When an eavesdropper (Eve) attempts to intercept the transmission, the no-cloning theorem ensures that the quantum

states collapse, leading to observable disturbances in the transmission and thereby revealing the presence of eavesdropping. After key exchange, error reconciliation and privacy amplification are performed to correct transmission errors and derive a secure, shared key between Bob and Alice [33].

2.3.3 Physical Layer Security (PLS)

Physical Layer Security of Free-Space Optical communication is focused on countering vulnerabilities like beam divergence, misalignment, and atmospheric turbulence to protect against unauthorized eavesdropping. Techniques like acousto-optic deflectors (AODs), synthetic holographic gratings, and orbital angular momentum multiplexing offer security by modifying beam characteristics. Experimental testbeds and modulation schemes like OOK and IM/DD quantify secrecy performance. Bessel-Gaussian beams and spatial light modulators increase resistance to turbulence, while hybrid FSO/RF systems and MIMO provide eavesdropping resistance. Other methods like secret key agreement (SKA) and optical data fragmentation provide resilience to security, thereby making PLS a vital field of study to protect FSO links [34].

2.3.4 Chaotic method

Chaotic signals are used in Free-Space Optical (FSO) communication to enhance security because they create complex, unpredictable waveforms that prevent eavesdropping. Their randomness makes data reconstruction impossible without exact system parameters, offering a dynamic and highly secure masking method, It function on both fronts to ensure secure FSO communication at the transmitter side for data encryption and at the receiver side for decryption accordingly [35]:

- **Transmitter side:**before the transmission, the data signal is mixed into a chaotic optical signal so that it becomes indistinguishable from random noise. This chaotic carrier acts as a protective shield, preventing unauthorized receivers from extracting meaningful information. Without the correct chaotic synchronization parameters, an attacker only gets a scrambled, meaningless signal.

- **Effect of Weather Conditions:** Weather conditions like haze, rain, and fog cause scattering and attenuation that have a negligible impact on the range of transmission. Chaotic masking ensures security nonetheless, with intercepted signals remaining un-

scramble. Security-versus-distance depends on the level of disturbances, with more intense disturbances weakening the signal.

- **Receiver side:** At the receiver end, a synchronized chaotic system is employed to eliminate the chaotic component of the signal from the input. This procedure recovers the original information, providing safe and precise restoration with no compromise in transmission efficiency.

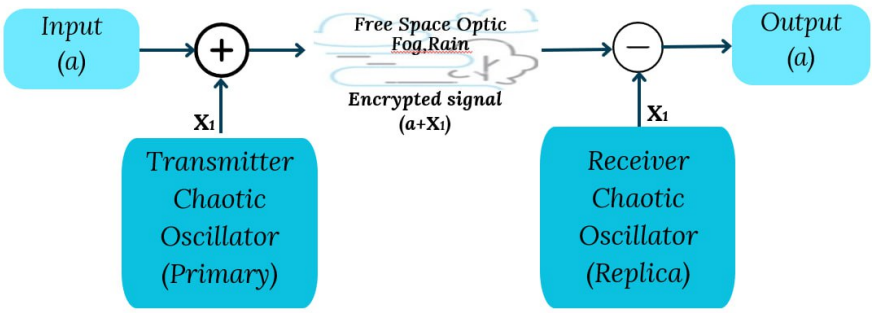


Figure 2.3: Block diagram of chaotic method.

2.4 Comparison of different encryption methods

Table 2.2 summarizes the different types of encryptions in terms of intended purpose, ease-of-use, and advantages and disadvantages. This comparison is a good start to understanding how each of the encryption types works, whether it is useful from a security perspective, and what potential weaknesses or challenges there might be in using that type of encryption.

Table 2.2: Comparison between different encryption methods.

Methods	Purpose	Advantages	Challenges
Choquet Fuzzy Integral (CFI), Integer Wavelet Transform (IWT)	Enhances security and clarity under adverse weather conditions.	- Robust pseudo-random encryption. - Reduces transmission errors. - Improves image quality in foggy environments.	- Performance affected by external conditions. - Additional processing overhead due to filtering and encryption.

Continued on next page

Methods	Purpose	Advantages	Challenges
Quantum Key Distribution (QKD)	Provides unconditional security using quantum mechanics.	- Nearly unbreakable encryption. - Eavesdropping detection via quantum state collapse.	- Requires specialized quantum hardware. - Sensitive to noise and photon loss in FSO channels.
Physical Layer Security (PLS)	Protects against beam spread, turbulence, and interception.	- Security based on physical properties. - Resilient imaging through Bessel-Gaussian beams and MIMO.	- Complex implementation. - Requires precise beam alignment and control.
Chaotic Method	Employs chaotic signals to hide data and prevent interception.	- Highly secure due to unpredictability. - Works effectively in extreme weather. - Information recovery is impossible without exact system parameters.	- Requires accurate synchronization between transmitter and receiver. - Atmospheric disturbances can degrade signal quality.

2.5 Chaotic Dynamical Systems

2.5.1 Dynamic System

Dynamic System is a mathematical description of the time development of some phenomenon. Dynamical systems are ubiquitous across most disciplines, from physics to engineering and biology, employing mathematical equations-continuous or discrete-to represent processes such as the motion of planets and the growth of populations. Some such systems can, in certain instances, portray chaotic behavior characterized by intricate and unpredictable dynamics [36]. As a special case, some dynamical systems exhibit very complicated and random-like behavior, which is referred to as chaos.

2.5.2 Chaotic System

Chaotic System is a dynamical system highly sensitive to initial conditions where slight changes can create vastly different outcomes. Unpredictable as they may be, these systems follow deterministic laws rather than randomness. They are nonlinear, complex, and non-classical mechanic, and because of this nature, long-term prediction is impossible [37].

2.5.3 Properties

Chaotic systems display complex dynamics, being governed by deterministic rules but leading to unpredictable behavior. Their characteristics are special and are required in encryption and secure communication in order to impart randomness and high security. The following are crucial characteristics that define chaotic systems:

- **Responsiveness to Initial Conditions:**Chaotic systems are extremely sensitive to initial conditions, and even slight differences in the initial state will give radically different results in the long term. Such as butterfly effect, as named by Edward Lorenz as showing in figure 2.4, makes long-term prediction impossible despite the determinism of the system. Chaos is investigated using dynamical systems, in which a system's state is defined by numerous time-dependent variables. Rather than dealing with these variables separately, it is preferable to visualize the system as a point that moves in an n-dimensional phase space, hence better understanding its evolution [38].

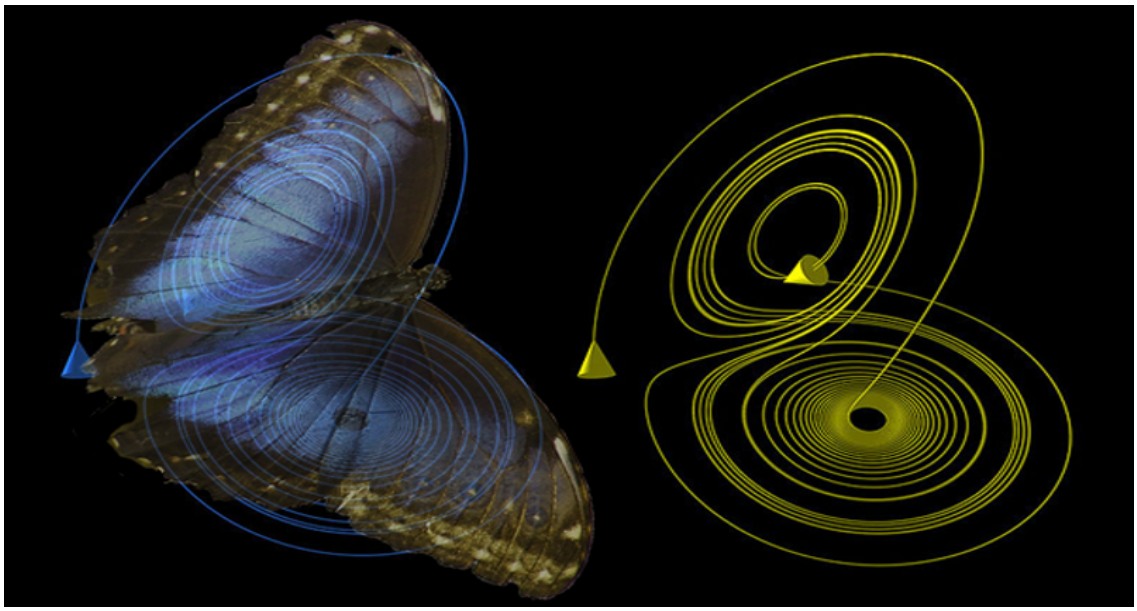


Figure 2.4: butterfly effect.

- **Unpredictability:** A chaotic system is unpredictable due to its instability and extreme sensitivity to initial conditions and parameters. A small change in starting values will cause a big change in coming states, and because of this, long-term prediction is virtually impossible [38].
- **Nonlinearity:** The governing equations are nonlinear, leading to complex dynamics.
- **Determinism:** The system evolves according to precise rules; the behavior is not random, even if it appears unpredictable.
- **Structured Irregularity:** The system possesses an infinite number of unstable periodic orbits, leading to seemingly disordered yet patterned behavior.

2.5.4 Chaos Vs Randomness

The main difference between chaos and randomness is based on their very foundation. Randomness is a result of inherent uncertainty, whereas chaos is due to sensitivity to initial conditions in deterministic systems. Chaotic action, although seemingly random in nature, is actually ruled by exact nonlinear equations, hence drawing a fundamental distinction with actual randomness [39].

2.5.5 Mathematical Models of Chaos

In order to comprehend chaotic behaviour, there exist various mathematical models that represent particular features of nonlinear dynamics. Prominent examples are the Lorenz system, Chua's circuit, and the Logistic Map, demonstrating how deterministic equations generate behaviour apparently random:

2.5.5.1 Lorenz system

The Lorenz model is a chaotic 3D system of atmospheric convection equations from which it follows the "butterfly effect", where the smallest initial changes induce the most significant long-term variations. The chaotic behaviour of the model is illustrated using methods such as differential equations and tools like strange attractors and bifurcations. The famous Lorenz chaotic system is defined as [40]:

$$\frac{dx(t)}{dt} = a(y(t) - x(t)) \tag{2.1}$$

$$\frac{dy(t)}{dt} = x(t)(c - z(t)) - y(t) \tag{2.2}$$

$$\frac{dz(t)}{dt} = x(t)y(t) - bz(t) \tag{2.3}$$

Where:

- a:is termed the Prandtl number.
- c:is termed the Rayleigh number.
- All a, b, c >0, but usually a = 10, b = 8/3, and c = 28.

2.5.5.2 Chua's circuit

Chua's circuit is a paradigmatic example of a nonlinear electronic system that exhibits rich dynamic behaviors, including bifurcations and chaos. It is one of the simplest physical circuits known to generate chaotic oscillations and is widely used in nonlinear dynamics research and secure communication systems.

As illustrated in Figure 2.5, Chua's circuit comprises a combination of linear and nonlinear electronic components:

- L: an inductor.
- R: nonlinear resistor;
- Ro is a small positive resistance of the inductor L.
- C1, C2: two capacitors.
- V1: the voltage across capacitor C1 and the nonlinear resistance.
- V2: the voltage across capacitor C2 and the voltage across the inductor.
- i3: the current through the inductor.
- NR: A nonlinear resistor called Chua's diode.

This nonlinear resistor NR is crucial, as it enables the circuit to generate chaotic behavior by introducing nonlinearity into the system [41]:

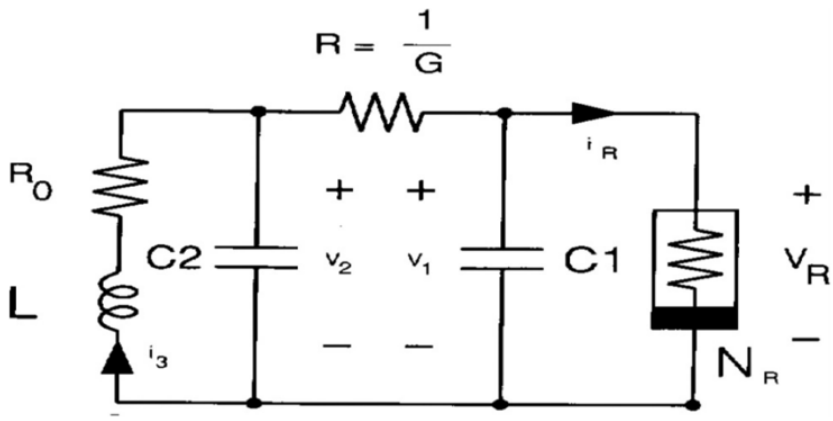


Figure 2.5: Chua's Circuit.

Electrical Analysis

Before deriving the mathematical model, fundamental electrical laws are applied:

- **Kirchhoff's Voltage Law (KVL)** in the loop including C_2, L, and R_0:

$$V_2 = L\frac{di_3}{dt} + R_0 i_3 \tag{2.4}$$

$$L\frac{di_3}{dt} = -V_2 + R_0 i_3 \tag{2.5}$$

- **Kirchhoff's Current Law (KCL)** at the node connecting C_1, C_2, and resistor R:

$$C_1\frac{dV_1}{dt} = \frac{1}{R}(V_2 - V_1) - i_R \tag{2.6}$$

  where $i_R = F(V_1)$

- Current through capacitor C2:

$$C_2\frac{dV_2}{dt} = \frac{1}{R}(V_1 - V_2) + i_3 \tag{2.7}$$

Dynamical Equations

The set of nonlinear differential equations governing Chua's circuit is:

$$C_1\frac{dV_1}{dt} = \frac{1}{R}(V_2 - V_1) - i_R \tag{2.8}$$

$$C_2\frac{dV_2}{dt} = \frac{1}{R}(V_1 - V_2) + i_3 \tag{2.9}$$

$$L\frac{di_3}{dt} = -(V_2 - R_0 i_3) \tag{2.10}$$

- The state curve presents the NR characteristic (figure 2.6):

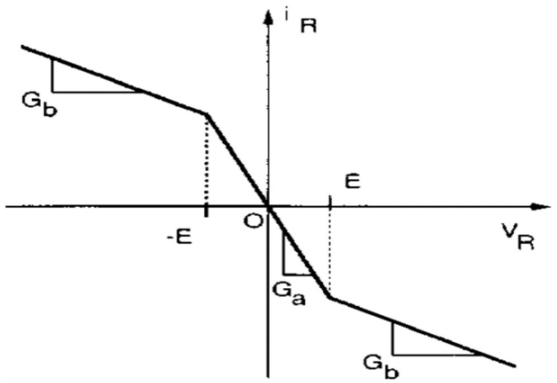


Figure 2.6: Characteristic of NR resistor.

The function F(V1) is presented by:

$$F(V_1) = G_b V_1 + \frac{1}{2}(G_a - G_b)\left(|V_1 + E| - |V_1 - E|\right) \tag{2.11}$$

Where:

- F(V1): non-linear voltage-current characteristic of the Chua' diode.
- Ga and Gb: negative conductances, they define the piecewise-linear segments:

- Ga: Inner slope (steeper or shallower, depending on parameters)
- Gb: Outer slope (usually more negative than Ga)

- E: the breakpoint voltage, it defines the locations (±E) where the slope of the V1 curve changes.

In order to facilitate analysis and carry out numerical simulations, the mathematical expressions for the system are rewritten in dimensionless form by introducing the following dimensionless options:

$$X_1 = \frac{V_1}{E}, X_2 = \frac{V_2}{E}, X_3 = \frac{R}{E} i_3, \tag{2.12}$$

$$\alpha = \frac{C_2}{C_1}, \beta = \frac{C_2 R^2}{L}, \gamma = \frac{R R_0 C_2}{L}, \tag{2.13}$$

$$a = R G_a, b = R G_b, \tag{2.14}$$

With these variable changes, the state equations are transformed into the form below:

$$\frac{dX_1}{dt} = \alpha(X_2 - X_1 - g(X_1)) \tag{2.15}$$

$$\frac{dX_2}{dt} = X_1 - X_2 + X_3 \tag{2.16}$$

$$\frac{dX_3}{dt} = \beta X_2 - \gamma X_3, \tag{2.17}$$

The effect of the nonlinear element g(X1) in the circuit is given by the nonlinear voltage-current characteristic of the Chua's diode, which is described by:

$$g(X_1) = bX_1 + \frac{1}{2}(a-b)\left(|X_1+1| - |X_1-1|\right) \tag{2.18}$$

Where:

- X1, X2 and X3: are the state variables.

- α, β, γ, a, b: are the system parameters.

2.5.5.3 Logistic Map

The Chaotic Logistic Map (CLM) is a dynamic system with certain significant features such as sensitivity to initial conditions, pseudo-randomness, good ergodicity, high efficiency, and high key space. It was first applied by Lorenz; all these features make it a possible candidate for quantum-safe image encryption algorithms. CLM is computationally efficient, uses simple hardware, and is easy to implement. It has been experimentally verified as a low-cost, high-speed encryption method, which makes it highly suitable for secure image processing and cryptographic applications. The governing equation for the logistic map is as follows [42]:

$$b_{n+1} = \gamma b_n(1 - b_n) \tag{2.19}$$

Where:

- b_n represents the population at time step n.

- γ(gamma) is the population growth rate.

- $1 - b_n$ represents the effect of limited resources (i.e., population constraints).

2.5.6 Application of chaos to cryptography

Chaos-based cryptography represents an innovative approach that leverages the complex dynamics of chaotic systems to enhance the security of communication. Due to their inherent unpredictability, extreme sensitivity to initial conditions, and pseudo-random behavior, chaotic systems are particularly well-suited for secure key generation and data encryption [38]. There are four main areas where chaos is applied in cryptographic systems:

- **Chaos-Based Cryptographic Systems:** Chaotic cryptographic systems utilize the intrinsic properties of chaotic dynamics to secure data transmission. These systems typically involve the following components:

  - A chaotic generator (scrambler): encrypts the message by embedding it into a chaotic signal;
  - A chaotic decryption system (descrambler): reconstructs the original message through chaotic synchronization;
  - Synchronization is essential: the transmitter and receiver must remain perfectly synchronized in their dynamic evolution to correctly recover the embedded message.

  These systems offer high sensitivity to initial conditions, pseudo-randomness, and complex structural behavior, making them particularly suitable for secure communication—especially in resource-constrained or high-speed environments.

- **Generation of Pseudo-Random Keys Using Chaos:**Chaotic systems can serve as pseudo-random number generators (PRNGs), which are fundamental in cryptographic operations. These PRNGs exploit the unpredictability of chaos to produce bit sequences that are difficult to reproduce. A common technique involves:

  - Generating floating-point numbers from chaotic equations (e.g., in double precision);
  - Applying a quantization function to derive binary cryptographic keys.

  Unlike truly random numbers, pseudo-random numbers are inherently periodic. However, the large parameter space and high sensitivity to initial conditions in chaotic systems make their outputs unpredictable and practically irreversible, which strengthens the cryptographic robustness.

A typical example includes mixing chaotic sequences with image data, ensuring that the generated key is strongly dependent on the system's initial state and parameters—thus enhancing unpredictability.

- **Chaos-Based Stream Ciphers:** Stream ciphers are encryption algorithms that rely on generating an infinite stream of cryptographic keys, used to encrypt data bit by bit or byte by byte. These ciphers require relatively low memory and are therefore highly efficient, particularly in embedded or real-time systems. The typical process involves:

  - A chaotic pseudo-random key stream generator;
  - Encryption of plaintext via XOR operations with the key stream.

  Stream ciphers are particularly effective when the plaintext size is unknown or when high performance is crucial. Their efficiency and simplicity make them ideal for high-speed encryption scenarios.

- **Chaos-Driven Block Cipher S-Boxes:** Substitution boxes (S-boxes) are critical nonlinear components in block cipher encryption, introducing confusion to enhance security. However, in digital image encryption, their use is often limited by high autocorrelation, especially between adjacent pixels, which can weaken the encryption against cryptanalytic attacks.

  To address this issue, researchers have developed dynamically driven chaotic S-boxes. These S-boxes are generated using chaotic maps that adapt to pixel correlations in images, thus significantly improving the resilience of image encryption schemes by introducing more complexity and less predictability into the transformation process.

2.6 Comparison between Classical Algorithms and Chaotic Encryption

Cryptography has progressed from classical mathematical approaches to modern methods, such as chaotic encryption, which utilizes nonlinear dynamic systems. Table 2.3 compares the difference between traditional cryptosystems and chaotic cryptosystems in relation to the operations performed, efficiency, and security [43].

Table 2.3: Different between Chaotic Cryptosystem and Traditional Cryptosystem.

Chaotic Cryptosystem	**Traditional Cryptosystem**
Operations of floating-point numbers	Operations of integer numbers
Slow working	Fast working
Nonlinear function can be anything	Primarily using the mod function
Don't require prime numbers	Primarily use prime numbers
Low cycle length	High cycle length
Has statistical biases	No statistical bias
Some data are useless	Some data are useful

In addition, table 2.4 investigates the relationship between chaos theory and cryptography, illustrating how traditional structured methods of cryptography contrast with the unpredictability of chaos. The comparison illustrates how using chaotic properties can increase cryptographic security.

Table 2.4: Relationship between Chaos Theory and Cryptography.

Chaos Theory	**Cryptography**
Chaotic cryptosystem	Pseudo-chaotic cryptosystem
Disordered operation	Disordered operation
Infinite stages	Finite stages
Infinite repetitions	Finite repetitions
Initial stage	Plain text
Final stage	Ciphertext
Initial conditions and/or parameters	Keys
Asymptotic independence of initial and final stages	Confusion

2.7 Advantages and challenges of chaotic encryption in FSO systems

Utilization of chaotic encryption on Free-Space Optical (FSO) communication has advantages and limitations which are:

Advantages:

- **High sensitivity to optical variations:** Chaotic encryption in FSO systems has a high sensitivity to optical channel variation. This makes it suitable for adapting to atmospheric disturbances like turbulence and temperature fluctuations, improving signal stability. By dynamically adjusting to changes in the optical path, chaotic encryption helps maintain signal integrity and enhances the reliability of data transmission in varying environmental conditions[44].

- **Robustness against attacks:** robustness against attacks in chaotic FSO systems, chaotic cryptographic techniques, such as the logistic maps. Those methods are meant to generate keys that cannot be foreseen or revealed and are resilient to the types of attacks that are known-plaintext, chosen-plaintext, statistical, and noise-based. FSO systems possess high entropies and key sensitivity, making it impossible for an unauthorized party to successfully decrypt information. It secures communication by stopping an unauthorized entity from performing decryption efficiently [45].

Challenges:

- **Synchronization:**Synchronization for chaotic encryption in FSO system is critical to recover a proper message. To obtain the actual signal receiver should perfectly emulate transmitter's chaotic behaviour. But turbulence and noise in atmosphere causing desynchronization degrades communication. Corrective measures requiring sophistication as well as fine controls are necessary to guarantee stability [46].

- **Hardware implementation:** Chaotic encryption is very complex to implement in Hardware with FSO systems. Optical amplifier is needed to overcome signal losses due to atmospheric attenuation during long-distance stable transmission. Even that, filters and signal processing units needed to be able dump the original message from the chaotic signal such that it can even be properly recovered of data. The additional components adds to higher charges and complexity of system, or demanding in terms of resources and technical considerations required for implementing this [46].

2.8 Conclusion

In general, this chapter points out the challenges of security in Free-Space Optical communication to propose chaotic signals as applicable solutions. FSO communication, although high-speed and interference-free, is however vulnerable to security threats, more so from atmospheric turbulence, that can seriously impair performance—especially in cases of 5G

network architectures. By using chaotic signals, we aspire to elevate secured communications by this means, notwithstanding future in-depth analysis regarding their effects upon overall performance of the system. The next chapter will undertake an investigation into this method's impact on FSO efficiency and reliability.

Chapter 3

Design and Simulation of secure FSO system

- **Contact Dr. Djellab Hanane regarding this chapter at the email address:** hanane.djellab@univ-tebessa.dz

General conclusion

Beginning with a foundational overview of 5G technologies and FSO systems, the research highlighted key advantages such as high throughput, low latency, and flexibility, while also addressing challenges like weather sensitivity and precise alignment. FSO systems were established as a strong candidate for high-capacity backhaul and temporary links within 5G infrastructure.

A detailed investigation into encryption techniques followed, comparing symmetric, asymmetric, quantum, and physical-layer security methods. Chaotic systems emerged as a particularly promising solution. The Chua circuit was selected for its simple implementation and ability to produce highly unpredictable keys with low computational overhead. Compared to classical encryption algorithms, chaotic encryption offers lightweight processing, inherent resistance to brute-force attacks, and robust key unpredictability.

To validate the proposed system, comprehensive simulations using `MATLAB` and `OptiSystem` were conducted. The architecture applied additive encryption and subtraction-based decryption using chaotic signals. It performed reliably under varying conditions:

- Data rates from 1 to 10 Gbps,
- Transmission distances up to 2 km,
- Atmospheric conditions from clear skies to dense fog (up to 8 dB/km).

Across all scenarios, the system consistently achieved a Bit Error Rate (BER) below 10^{-6}, surpassing the performance of non-secure FSO systems in terms of BER, Q-factor, and eye diagram clarity—indicative of improved signal integrity and robustness.

The system also underwent rigorous cryptographic evaluation, confirming its high sensitivity (MSE = 0.518), strong entropy ($H = 0.99943$), vast key space ($\sim 3.09 \times 10^{39}$), and positive Lyapunov exponent ($\lambda \approx 0.648$)—affirming its chaotic and secure nature. Furthermore, a comparative analysis under varying atmospheric conditions (clear, foggy, snowy) revealed that the secure FSO system extends the transmission range by 300–400 meters

compared to its non-secure counterpart, owing to enhanced signal resilience and synchronization robustness. **In summary**, this research demonstrates that chaotic encryption not only strengthens the security of FSO systems but also enhances their transmission reliability. Its efficiency, adaptability, and resilience position it as a promising approach for safeguarding 5G optical wireless communications.

Bibliography

[1] M. Alsharari, K. Aliqab, F. Ali, and A. Armghan, "Integrated free-space optics and fiber optic network performance enhancement for sustaining 5g high capacity communications," *International Journal of Optics*, vol. 2023, no. 1, p. 8685686, 2023.

[2] C. Li, J. Shi, Q. Liu, H. Tu, Z. Lei, C. Yang, and J. Yao, "Crystal growth and property characterization of a novel long-wave infrared nonlinear optical crystal bahggese4," *Crystal Growth & Design*, vol. 24, no. 22, pp. 9804–9809, 2024.

[3] W. Alheadary, *Free Space Optics for 5G Backhaul Networks and Beyond*. Phd thesis, King Abdullah University of Science and Technology (KAUST), August 2018.

[4] S. V. K. Eguri, A. B. Raj A, and N. Sharma, "Survey on acquisition, tracking and pointing (atp) systems and beam profile correction techniques in fso communication systems," *Journal of Optical Communications*, vol. 45, no. 4, pp. 881–904, 2024.

[5] S. A. Al-Gailani, M. F. Mohd Salleh, A. A. Salem, R. Q. Shaddad, U. U. Sheikh, N. A. Algeelani, and T. A. Almohamad, "A survey of free space optics (fso) communication systems, links, and networks," *IEEE Access*, vol. 9, pp. 7353–7373, 2021.

[6] E. Farooq, A. Sahu, and S. K. Gupta, "Survey on fso communication system—limitations and enhancement techniques," in *Lecture Notes in Electrical Engineering*, pp. 255–264, Springer, 2018.

[7] S. Kumar and N. Sharma, "Emerging military applications of free space optical communication technology: A detailed review," in *Journal of Physics: Conference Series*, vol. 2161, p. 012011, IOP Publishing, 2022.

[8] S. S. Patil, C. Joseph, D. Varpe, and A. B. Raj, "A comprehensive review on security in free space optical communication," *International Journal of Engineering Research and Reviews*, vol. 12, no. 3, pp. 150–180.

[9] H. Singh, N. Mittal, R. Miglani, H. Singh, G. S. Gaba, and M. Hedabou, "Design and analysis of high-speed free space optical (fso) communication system for supporting fifth generation (5g) data services in diverse geographical locations of india," *IEEE Photonics Journal*, vol. 13, no. 5, pp. 1–12, 2021.

[10] I. A. Alimi and P. P. Monteiro, "Revolutionizing free-space optics: A survey of enabling technologies, challenges, trends, and prospects of beyond 5g free-space optical (fso) communication systems," *Sensors (Basel, Switzerland)*, vol. 24, no. 24, p. 8036, 2024.

[11] D. MOKHTAR, *ETUDE ET EVALUATION DES PERFORMANCES D'UN SYSTEME DE COMMUNICATION SAC-OCDMA DANS LES LIAISONS FSO*. PhD thesis, Faculté des Sciences et Technologies, 2021.

[12] Y. Ma, Q. Chen, S. Wang, S. Sharma, and S. Khanna, "Retracted: Research on dispersion compensation using avalanche photodiode and pin photodiode," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 205–214, 2021.

[13] A. F. NOUN Amina, "Etude et analyse des performances du système wdm/fso," 2021.

[14] O. Aboelala, I. E. Lee, and G. C. Chung, "A survey of hybrid free space optics (fso) communication networks to achieve 5g connectivity for backhauling," *Entropy*, vol. 24, no. 11, p. 1573, 2022.

[15] A. S. Madhuri, G. Immadi, V. Mounika, A. TarunTeja, T. Aakash, and N. S. Srinivasa, "Performance evaluation of free space optics using different modulation techniques at various link ranges," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, pp. 834–838, April 2019.

[16] O. O. Erunkulu, A. M. Zungeru, C. K. Lebekwe, M. Mosalaosi, and J. M. Chuma, "5g mobile communication applications: A survey and comparison of use cases," *IEEE Access*, vol. 9, pp. 97251–97295, 2021.

[17] Y. M. Azzedine Marwa, "Architecture et transmission de l'information dans les réseaux radio-mobiles 5g," 2021.

[18] A. Amphawan, N. Arsad, T.-K. Neo, M. B. Jasser, and A. Mohd Ramly, "Post-flood uav-based free space optics recovery communications with spatial mode diversity," *Electronics*, vol. 11, no. 14, p. 2257, 2022.

[19] X. Zhao, H. Askari, and J. Chen, "Nanogenerators for smart cities in the era of 5g and internet of things," *Joule*, vol. 5, no. 6, pp. 1391–1431, 2021.

[20] S. A. Dange, S. B. Patil, V. T. Patil, S. S. Mulla, and A. S. Husainy, "A review on 5g technology: Evolution, features and challenges," *Asian Journal of Science and Applied Technology*, vol. 10, no. 2, pp. 15–21, 2021.

[21] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5g: Ran, core network and caching solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3098–3130, 2018.

[22] I. Sousa, N. Sousa, M. P. Queluz, and A. Rodrigues, "Fronthaul design for wireless networks," *Applied Sciences*, vol. 10, no. 14, p. 4754, 2020.

[23] L. Ndiaye, S. Diouf, K. Gueye, and S. Ouya, "Proposal for a deployment of a non-standalone 5g mobile network architecture for developing countries: Case of senegal," in *Interactive Mobile Communication, Technologies and Learning*, pp. 342–360, Springer, 2021.

[24] D. Neves, A. Sanches, R. Nobrega, H. Mrabet, I. Dayoub, K. Ohno, S. Haxha, I. Glesk, A. Jurado-Navas, and T. Raddo, "Beyond 5g fronthaul based on fso using spread spectrum codes and graphene modulators," *Sensors*, vol. 23, no. 8, p. 3791, 2023.

[25] H. A. Fadhil, H. Y. Ahmed, M. Zeghid, and W. A. Imtiaz, "High attitude platform free space optics system using various filtering operations for fifth generation system," *Optical and Quantum Electronics*, vol. 53, no. 8, p. 475, 2021.

[26] S. T. Hayle, H.-Y. Hsu, C.-P. Wang, H.-H. Lu, J.-M. Lu, W.-W. Hsu, Y.-C. Chung, Y.-Y. Bai, and K. Okram, "High-speed fso-5g wireless communication system with enhanced loss compensation using high-power edfa," *Scientific Reports*, vol. 15, no. 1, p. 379, 2025.

[27] N. Alshaer, A. Moawad, and T. Ismail, "Reliability and security analysis of an entanglement-based qkd protocol in a dynamic ground-to-uav fso communications system," *IEEE Access*, vol. 9, pp. 168052–168067, 2021.

[28] A. K. Bermani, T. A. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1613–1624, 2021.

[29] P. Matta, M. Arora, and D. Sharma, "A comparative survey on data encryption techniques: Big data perspective," *Materials today: proceedings*, vol. 46, pp. 11035–11039, 2021.

[30] P. Abos, "Encryption and key management: Robust encryption techniques and secure key management systems," may 2024.

[31] S. A. Abd El-Mottaleb, A. G. Mohamed, H. Y. Ahmed, and M. Zeghid, "Performance enhancement of fso communication system under rainy weather environment using a novel encryption technique," *IEEE Access*, vol. 12, pp. 13729–13746, 2024.

[32] S. A. Abd El-Mottaleb, A. G. Mohamed, A. Chehri, M. Singh, A. Atieh, H. Y. Ahmed, and M. Zeghid, "Performance of cipher image transmission in free space optics under foggy weather," *IEEE Access*, vol. 11, pp. 139478–139497, 2023.

[33] B. Mallick, P. Parida, C. Nayak, P. K. Sahoo, and G. Palai, "Quantum key distribution over fso channel using error reconciliation protocol," *Wireless Networks*, vol. 29, no. 5, pp. 2161–2169, 2023.

[34] W. Shakir and R. Abdulkareem, "A survey on physical layer security for fso communication systems," in *Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST*, pp. 7–9, 2021.

[35] E. Fadil, A. Abass, and S. Tahhan, "Secure wdm-free space optical communication system based optical chaotic," *Optical and Quantum Electronics*, vol. 54, no. 8, p. 477, 2022.

[36] R. Y. Franco, "Cryptographie vidéo par le système chaotique utilisant la suite logistique," mémoire de master, antananarivo.

[37] O. Rabiaa, "Systèmes dynamiques et chaos: Différentes méthodes de contrôle et de synchronisation," *Université frères mentouri Constantine*, vol. 1, 2018.

[38] K. A. Korba, *La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques*. PhD thesis, Université 08 mai 45 Guelma (Algérie), 2022.

[39] F. Hachouf and D. E. Goumidi, "Fonction logique et standard chaotique pour le chiffrement des images satellitaires," 2014. Disponible en ligne : https://archives.umc.edu.dz/handle/123456789/5869.

[40] I. Petráš, "The fractional-order lorenz-type systems: A review," *Fractional Calculus and Applied Analysis*, vol. 25, no. 2, pp. 362–377, 2022.

[41] F. Maamri, S. Bououden, and I. Boulkaibet, "Identification of chua's chaotic circuit parameters using penguins search optimisation algorithm," *Cyber-Physical Systems*, vol. 8, no. 3, pp. 233–260, 2022.

[42] M. Riaz, H. Dilpazir, S. Naseer, H. Mahmood, A. Anwar, J. Khan, I. B. Benitez, and T. Ahmad, "Secure and fast image encryption algorithm based on modified logistic map," *Information*, vol. 15, no. 3, p. 172, 2024.

[43] P. K. Shukla, A. Khare, M. A. Rizvi, S. Stalin, and S. Kumar, "Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing," *Entropy*, vol. 17, no. 3, pp. 1387–1410, 2015.

[44] A. Niaz, F. Qamar, M. Ali, R. Farhan, and M. K. Islam, "Performance analysis of chaotic fso communication system under different weather conditions," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 2, p. e3486, 2019.

[45] J. Oravec, J. Turán, L. Ovseník, and T. Huszaník, "A chaotic image encryption algorithm robust against the phase space reconstruction attacks," *Acta Polytech. Hung*, vol. 16, no. 3, pp. 37–57, 2019.

[46] M. M. Sepantaie, N. M. Namazi, and A. M. Sepantaie, "Spectral analysis and implementation of secure chaotic free-space optical communication systems," *Optical Engineering*, vol. 57, no. 10, pp. 106101–106101, 2018.

[47] J. Yang and L. Zhao, "Bifurcation analysis and chaos control of the modified chua's circuit system," *Chaos, Solitons & Fractals*, vol. 77, pp. 332–339, 2015.

[48] M. H. Shaligram and P. K. Bajaj, "Performance evaluation of free space optical communication system," 2023.