WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Development and Evolution of Cryptographic Algorithms in Response to Cyber Threats.

[1]Chris Gilbert, [2]Mercy Abiola Gilbert

[1]Professor [2]Instructor

[1]Department of Computer Science and Engineering/College of Engineering and Technology/William V.S. Tubman University/chrisgilbertp@gmail.com/cabilimi@tubmanu.edu.lr

[2]Department of Guidance and Counseling/College of Education/William V.S. Tubman University/mercyabiola92@gmail.com/moke@tubmanu.edu.lr

DOI : https://doi.org/10.55248/gengpi.5.1224.3430

ABSTRACT

The evolution of cryptographic algorithms has been essential in responding to the growing threats in the digital age. This paper examines the development of cryptography, starting with ancient methods like the Caesar cipher, and leading to modern algorithms such as RSA, AES, and the emerging field of post-quantum cryptography. Through detailed analysis, including a review of existing literature, case studies, and mathematical modeling, the paper explores how cryptographic techniques have adapted to secure data against increasingly sophisticated cyberattacks. It also addresses vulnerabilities in current systems, such as brute-force and side-channel attacks, and considers the looming threat of quantum computing, which could compromise widely used encryption methods. Finally, the paper looks ahead to new innovations like homomorphic encryption and AI-driven cryptographic solutions, emphasizing the need for ongoing research and development to stay ahead of evolving cyber threats.

Keywords: *cryptography, RSA, AES, quantum computing, cyber security, encryption, side-channel attacks, post-quantum cryptography, homomorphic encryption, AI in cryptography.*

1. Introduction

The evolution of cryptographic research began in response to the increasing complexities of modern networking environments, particularly with the transmission of data over wireless media. This evolution addressed various challenges such as data security and the mitigation of attacks on cryptographic algorithms. The growth of cyber attackers, driven by advances in digital technologies, computers, and communication networks, has necessitated the continual development of cryptographic algorithms. Numerous advancements in algorithm design have been achieved through extensive research, providing a robust foundation for data security (Rao Peechara, 2021).

With the rise in internet usage for personal communication, banking, and various online services, the need for secure information transfer has become paramount. Modern secure communication systems rely heavily on cryptography, with the primary goal being the safeguarding of data during transmission. Central to this process are the concepts of encryption and decryption. Encryption converts plain text into unreadable cipher text using an algorithm, while decryption reverses the process, restoring the original plain text from the cipher text. These methods are critical for ensuring that sensitive information remains protected during data transfer (Henson & Taylor, 2014; Irviani & Muslihudin, 2018; Yeboah, Opoku-Mensah & Abilimi, 2013a).

1.1. Background and Significance

To ensure adequate security in the face of modern cyber threats, it is essential to continually develop new cryptographic algorithms. This necessity has led to ongoing discussions about the appropriate use of encryption in various network settings (Baseri, Chouhan & Hafid, 2024; Gilbert & Gilbert, 2024a; Yeboah, Odabi & Abilimi Odabi, 2016). The primary reason for this evolution lies in the fact that widely-used cryptosystems are based on fundamental computational operations, such as multiplication, addition, and exponentiation. For these systems to be efficient, they require modern computational structures. Furthermore, threats arise when input patterns, encrypted using error-detection-and-correction schemes, present vulnerabilities. A key issue in this context is that several encryption systems, particularly those involving keys or public key encryptions, rely on prime numbers, finite fields, or finite groups. These systems are highly sensitive to abstract operations, such as factorization, which affects the integrity of the encryption processes tied to these algebraic structures.

Today, cryptographic techniques are primarily divided into two categories: symmetric and asymmetric. In symmetric key cryptography, the same key is used for both the encryption and decryption processes. However, asymmetric techniques were introduced to address some limitations of symmetric key methods. In asymmetric cryptosystems, each entity possesses two distinct keys—one public and one private (Talukder et al., 2023; Opoku-Mensah, Abilimi & Amoako, 2013). Standardized asymmetric key techniques, which ensure confidentiality, digital signatures, and secure key exchange, include widely recognized protocols like RSA, ElGamal, and the Diffie-Hellman key exchange.

Cryptographic algorithms consist of controlled operations designed to deliver essential security services in open network environments. These services include ensuring confidentiality, maintaining data integrity, confirming provenance, guaranteeing accessibility, and providing non-repudiation assurances. As new vulnerabilities are discovered in older encryption methods, the field of cryptography continues to evolve, with new encryption and hash algorithms regularly being proposed to replace flawed systems (Henson & Taylor, 2014; Gilbert & Gilbert, 2024t).

1.2. Research Objectives

The potential outcomes of attacks on cryptographic systems often include the identification or determination of private keys, which are crucial for message authentication, key exchange, and the encryption/decryption process. Additionally, variations of these ciphers have been developed to safeguard against side-channel attacks, which target the underlying cryptographic operations. Another area of concern involves time-based threats, such as fluctuations in the ability to compromise public or private key operations. While this introduction touches on these topics, a detailed examination of Electromagnetic Side-Channel Analysis (EM-SCA) assaults across the evolution of cryptographic algorithms is beyond the scope of this discussion. Instead, a brief historical overview is provided on the development and mitigation of threats posed by electromagnetically-assisted attacks on cryptographic applications.

Cryptographic algorithms are employed to protect data and communications (Smrčka et al., 2023; Kwame, Martey & Chris, 2017; Gilbert & Gilbert, 2024o). However, the use of these encoding mechanisms does not make them immune to attacks; rather, they have become increasingly sophisticated over time. One form of attack on cyber systems, particularly those involving hardware or chip-based systems, involves exploiting software through electromagnetic emissions or fluctuations captured from side channels, including power, temperature, timing, and error signals (Zunaidi, Sayakkara & Scanlon, 2024; Gilbert & Gilbert, 2024p). EM-SCA is a prime example of such hardware-assisted offline cyberattacks. This type of assault collects electromagnetic emissions from parallel power supply lines or other potential sources to evaluate various cryptographic random functions. This paper focuses on the development of "Stream Ciphers" and "Block Cipher" cryptographic algorithms, which are targeted by EM-SCA attacks through byte-wise, block-wise, and bit-wise techniques in the electromagnetic and thermal spectrum.

1.3 Research Approaches and Method used

Literature Review

The literature review forms the backbone of the paper by examining both historical and modern advancements in cryptography. It references key research, such as the development of RSA, Diffie-Hellman, ElGamal, and AES algorithms, providing an understanding of how cryptographic techniques have evolved in response to increasing cyber threats. The review highlights the necessity of continuous advancements to maintain data security and identifies gaps in existing methods that have driven the creation of new encryption solutions.

Documentary Research

The research uses historical documents and technical standards to track the progression of cryptographic algorithms. For example, the development of the Data Encryption Standard (DES) by IBM in 1972, the AES competition organized by NIST, and the Federal Information Processing Standards (FIPS) are analyzed. These sources offer insights into how cryptography has adapted over time to address changing security needs and technological advancements.

Algorithmic Analysis

This method is applied to assess the strengths and weaknesses of various cryptographic algorithms. The paper compares symmetric and asymmetric encryption techniques like RSA, ECC, and AES, focusing on their key lengths, computational demands, and security measures. It also explores how these algorithms perform in different environments, such as IoT networks and in the face of quantum computing, to understand their effectiveness against modern cyberattacks.

Case Studies

Case studies are used to demonstrate the practical application of cryptographic techniques in real-world scenarios. For instance, the paper discusses the use of cryptography in healthcare systems during the COVID-19 pandemic, focusing on how encryption has been applied to secure electronic health records (EHRs). These examples highlight the importance of cryptography in securing sensitive information across industries.

Mathematical Modeling

The paper explores the mathematical foundations of cryptographic algorithms such as RSA, ECC, and AES. It explains the key mathematical principles like prime factorization and elliptic curves, which are crucial for generating encryption keys and ensuring algorithm security. The modeling also illustrates the computational difficulty of breaking these encryption methods, while discussing how quantum computing may challenge their security.

Threat Analysis

Threat analysis focuses on identifying the vulnerabilities in cryptographic systems and the attacks that exploit them, such as brute-force, side-channel, and quantum-based attacks. The research evaluates how these attacks work to undermine encryption and discusses countermeasures to mitigate these risks. This analysis underscores the ongoing need to develop stronger cryptographic defenses against emerging threats.

Trend Analysis

The paper examines emerging trends in cryptography, such as the development of post-quantum cryptography, homomorphic encryption, and blockchain-based security (Gilbert & Gilbert, 2024a). It explores how advances in quantum computing and artificial intelligence are reshaping cryptographic research, necessitating the creation of algorithms that can withstand quantum-level attacks. The analysis also highlights global efforts to standardize quantum-resistant encryption methods.

Theoretical Projection

Theoretical projections in the paper explore the future of cryptography in light of quantum computing and biometric encryption. The research anticipates scenarios in which traditional encryption methods like RSA and ECC may become vulnerable, advocating for the adoption of post-quantum cryptography. It also examines the potential role of AI and machine learning in shaping future cryptographic solutions and cybersecurity frameworks.

Simulation

While not heavily detailed, the paper implies that simulation techniques are essential for testing new cryptographic algorithms, especially in the context of quantum computing. These simulations are crucial for validating post-quantum cryptographic methods and modeling how algorithms will behave under quantum-based attacks, ensuring that they remain resilient to future cyber threats.

This comprehensive approach highlights the application of diverse research methods to investigate the evolution of cryptographic algorithms and their response to the ever-evolving landscape of cyber threats (see ***Figure 1***).

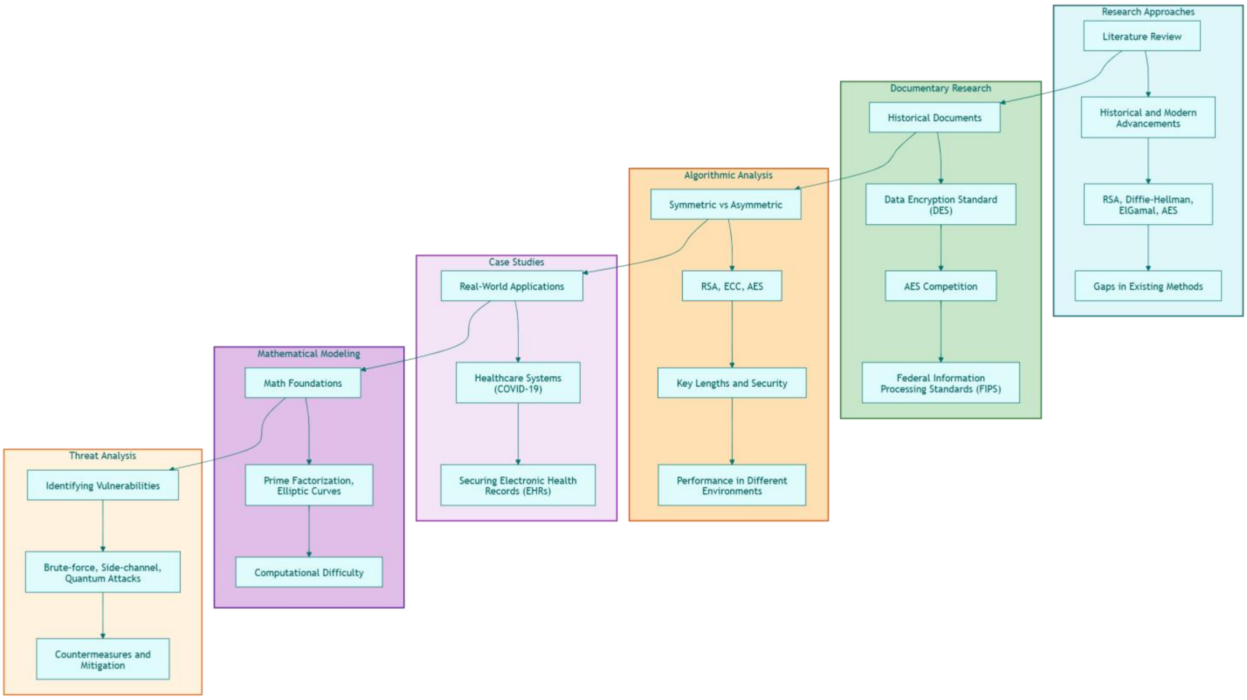
Research Approaches
Literature Review
Historical and Modern Advancements
RSA, Diffie-Hellman, ElGamal, AES
Gaps in Existing Methods
Documentary Research
Historical Documents
Data Encryption Standard (DES)
AES Competition
Federal Information Processing Standards (FIPS)
Algorithmic Analysis
Symmetric vs Asymmetric
RSA, ECC, AES
Key Lengths and Security
Performance in Different Environments
Case Studies
Real-World Applications
Healthcare Systems (COVID-19)
Securing Electronic Health Records (EHRs)
Mathematical Modeling
Math Foundations
Prime Factorization, Elliptic Curves
Computational Difficulty
Threat Analysis
Identifying Vulnerabilities
Brute-force, Side-channel, Quantum Attacks
Countermeasures and Mitigation

Figure 1: **The outlines of various research approaches to cryptography**

2. Historical Overview of Cryptography

In 1972, a team from IBM introduced the Data Encryption Standard (DES), marking a significant milestone as the first widely adopted secure block cipher. The primary objective behind DES was to increase the cipher's key length to a "communally acceptable war length" that could only be feasibly cracked by U.S. government intelligence agencies, while remaining secure against other potential adversaries. Over the last two decades, cryptographic algorithms have advanced, establishing security levels of 112 bits or greater, which has now become the standard for high-security environments. The Federal Information Processing Standard (FIPS 140-2) outlines various security levels for symmetric encryption algorithms, categorizing them into levels 1 through 4, with key lengths of 112, 128, 192, and 256 bits, respectively (El-Dalahmeh et al., 2024; Yeboah, Opoku-Mensah & Abilimi, 2013b; Gilbert & Gilbert, 2024q).

The development and evolution of cryptographic algorithms have played a pivotal role in addressing the growing security threats in cyber systems. The history of cryptography spans thousands of years, from the era of Caesar ciphers to the modern internet. As the internet and advancements in key distribution evolved, classical computing became increasingly vulnerable, rendering traditional methods inadequate for maintaining privacy and data security (Gilbert & Gilbert, 2024f). With sufficient knowledge, adversaries could bypass encryption and gain unauthorized access to data, leading to the development of more secure systems, particularly post-quantum cryptography. Although post-quantum cryptography offers enhanced security, especially through optical communication channels, its high cost places it outside the immediate focus of this chapter (Raeisi-Varzaneh et al., 2024; Gilbert & Gilbert, 2024g; Opoku-Mensah, Abilimi & Boateng, 2013). See figure below:

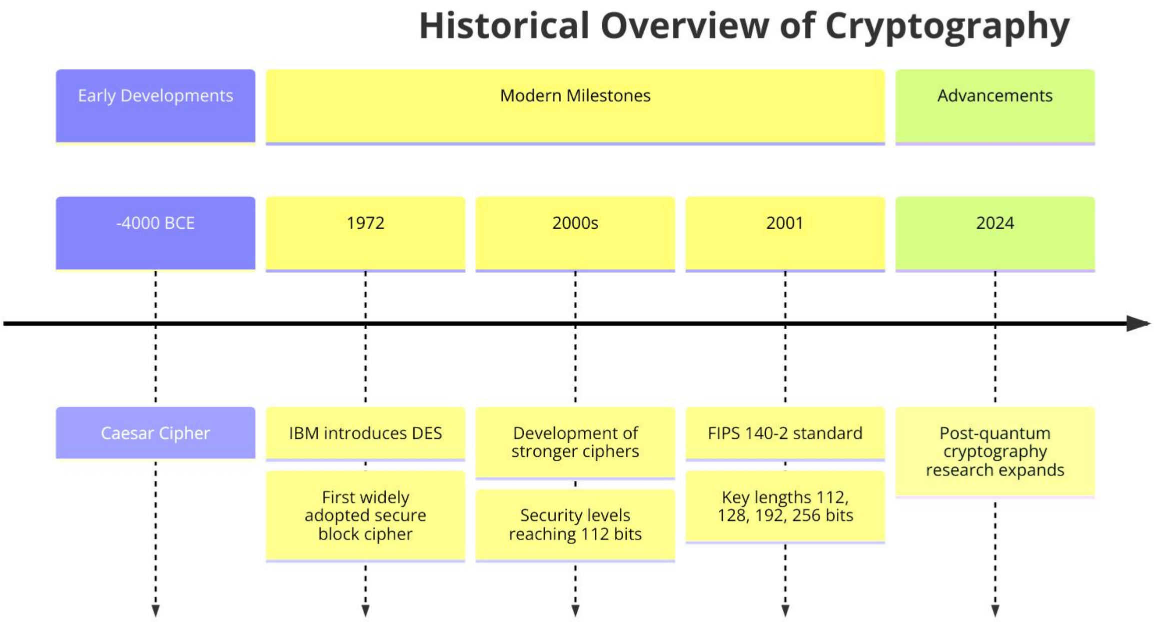
Historical Overview of Cryptography
Early Developments
Modern Milestones
Advancements
-4000 BCE
1972
2000s
2001
2024
Caesar Cipher
IBM introduces DES
First widely adopted secure block cipher
Development of stronger ciphers
Security levels reaching 112 bits
FIPS 140-2 standard
Key lengths 112, 128, 192, 256 bits
Post-quantum cryptography research expands

Figure 2: **Historical Overview of Cryptography**

2.1. Ancient Cryptography Techniques

Encryption is the process of transforming original data into a format that is unrecognizable to unauthorized entities. This transformation plays a crucial role in ensuring information security. One of the earliest encryption methods is the Caesar cipher, which involves replacing each letter in a text with another letter a fixed number of spaces forward in the alphabet. This method, known as a classical encryption algorithm, is symmetric, meaning it uses a single key for both encryption and decryption. Another ancient method is the scytale, where both the encryption and decryption processes are performed using the same key. In this method, the message is wrapped around a cylinder, shifting the alphabet in a way that distorts the original text (Vyakaranal & Kengond, 2018; Gilbert & Gilbert, 2024r).

Cryptographic techniques have been used for centuries to protect sensitive information, but the advent of electronic computers and localized networking marked a new stage in cryptography's evolution. In this era, early ciphers like DES and RSA began to dominate the field of security (Khan & Chishti, 2020; Gilbert & Gilbert, 2024s). These early ciphers were developed for a different technological environment, where the limited computing power of the time restricted the length and complexity of encryption keys. As a result, the encryption keys used during this period were relatively small compared to the more robust keys required by today's advanced computing capabilities.

A Mathematical Model of the Caesar Cipher

Understanding the Caesar Cipher

The Caesar cipher is a simple substitution cipher where each letter in the plaintext is shifted a fixed number of positions down the alphabet. For instance, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on.

Mathematical Representation

Let's represent each letter in the alphabet as a number:

- A = 0
- B = 1
- ...

- Z = 25

Let P be the plaintext message, C be the ciphertext, and k be the shift value.

The encryption process can be represented as a modular arithmetic operation:

$C(i) = (P(i) + k) \bmod 26$

Where:

- $C(i)$ is the ith character of the ciphertext
- $P(i)$ is the ith character of the plaintext
- k is the shift value

Decryption

Decryption is the reverse process:

$P(i) = (C(i) - k) \bmod 26$

Limitations of the Caesar Cipher

While simple to implement, the Caesar cipher is highly vulnerable to attacks, particularly frequency analysis. By analyzing the frequency distribution of letters in the ciphertext, an attacker can often deduce the shift value and decrypt the message.

Mathematical Model for the Scytale Cipher

Understanding the Scytale Cipher

The Scytale cipher is a transposition cipher, where the plaintext is wrapped around a cylinder (the scytale) and read off row by row. The decryption process involves wrapping the ciphertext around a scytale of the same diameter.

Mathematical Representation

While the Scytale cipher doesn't directly involve complex mathematical operations, we can represent the process using a matrix-based approach:

Encryption:

1. **Step 1: Transposition:** Convert the plaintext into a matrix, row by row, filling the matrix column-wise. The number of columns in the matrix is determined by the circumference of the scytale.
2. **Step 2: Read-off:** Read the ciphertext by traversing the matrix row by row.

Decryption:

1. **Step 1: Transposition:** Write the ciphertext into a matrix, row by row, with the same number of columns as the encryption matrix.
2. **Step 2: Read-off:** Read the plaintext by traversing the matrix column by row.

Limitations of the Scytale Cipher

While the Scytale cipher was effective in its time, it has significant limitations:

- **Limited Key Space:** The key is simply the diameter of the scytale, limiting the number of possible keys.
- **Vulnerability to Frequency Analysis:** Even though the order of letters is changed, the frequency distribution of letters remains the same, making it susceptible to frequency analysis attacks.

Modern Cryptography

Modern cryptographic techniques, such as public-key cryptography and symmetric-key cryptography, offer much stronger security than ancient ciphers. These techniques rely on complex mathematical algorithms and computational difficulty to ensure the confidentiality and integrity of data(Gilbert, 2012).

Key Differences between Ancient and Modern Cryptography:

- **Key Length:** Ancient ciphers often used short keys, making them vulnerable to brute-force attacks. Modern cryptography uses much longer keys, making it computationally infeasible to break.
- **Computational Complexity:** Modern cryptography relies on computationally intensive algorithms, such as those based on prime factorization or discrete logarithms, which are difficult to solve.

- **Mathematical Foundations:** Modern cryptography is built on solid mathematical foundations, including number theory, algebra, and probability theory.

2.2. Modern Cryptography Techniques

Over the years, we've seen the evolution of multiple generations of cellular hardware suites. A significant challenge in this development has been the limitation of cryptographic key sizes, primarily due to hardware inadequacies (Gill et al.,2024). As a result, efforts have focused on conducting cryptanalysis of the underlying hardware block designs to improve cryptographic resilience. While NIST is currently conducting the third round of the post-quantum cryptography challenge, there has also been a push towards developing more flexible cryptographic systems, particularly by designing our own encryption suites (Sedghighadikolaei & Yavuz, 2023; Gilbert & Gilbert, 2024t).

Polymorphic ciphers, such as Kreyvium and Simon, have been the subject of considerable development, with a focus on lightweight ciphers that optimize energy consumption. These ciphers are increasingly used in both stream and block cipher implementations, which are essential for secure communication streams. The research into post-quantum cryptographic algorithms is particularly important, given the potential threat posed by quantum technologies (Gilbert & Gilbert, 2024b; Yalamuri, Honnavalli & Eswaran, 2022; Abilimi & Adu-Manu, 2013). However, the proliferation of multi-standard IoT scenarios has made it cumbersome to carry separate cryptographic keys for each communication. This has highlighted the need for a diversified approach to cryptographic methods that can adapt to varying conditions (Gilbert & Gilbert, 2024k).

After NIST and other organizations standardized algorithms like RSA and ECC, these technologies became widely adopted (Patel et al., 2023; Abilimi & Yeboah, 2013). For example, RSA became a staple in digital certificates, and its 4100-bit key was finalized in 1996. However, over time, Elliptic Curve Digital Signature Algorithm (ECDSA) outperformed RSA due to advancements in elliptic curve cryptography (ECC), which provided greater security and efficiency with smaller key sizes (Gilbert & Gilbert, 2024m). ECC proved to be particularly advantageous, offering enhanced confidentiality and security while being less vulnerable to key compromise.

Modern cryptographic techniques continue to evolve. Trends in cryptanalysis are pushing the boundaries of traditional cryptographic algorithms, providing valuable guidance for research and system builders(Park et al.,2021). The foundational elements of modern cryptographic algorithms include symmetric key encryption, public-key encryption, hash functions, and digital signatures. After the 1970s, many symmetric and asymmetric key cryptographic algorithms were submitted to NIST for evaluation. Of the 57 submissions for the Advanced Encryption Standard (AES) competition, five finalists were selected—MARS, RC6, Rijndael, RC5, and Serpent—with Rijndael ultimately becoming the standard AES algorithm (Radanliev & De Roure, 2023).This shown in Figure 3 and 4.

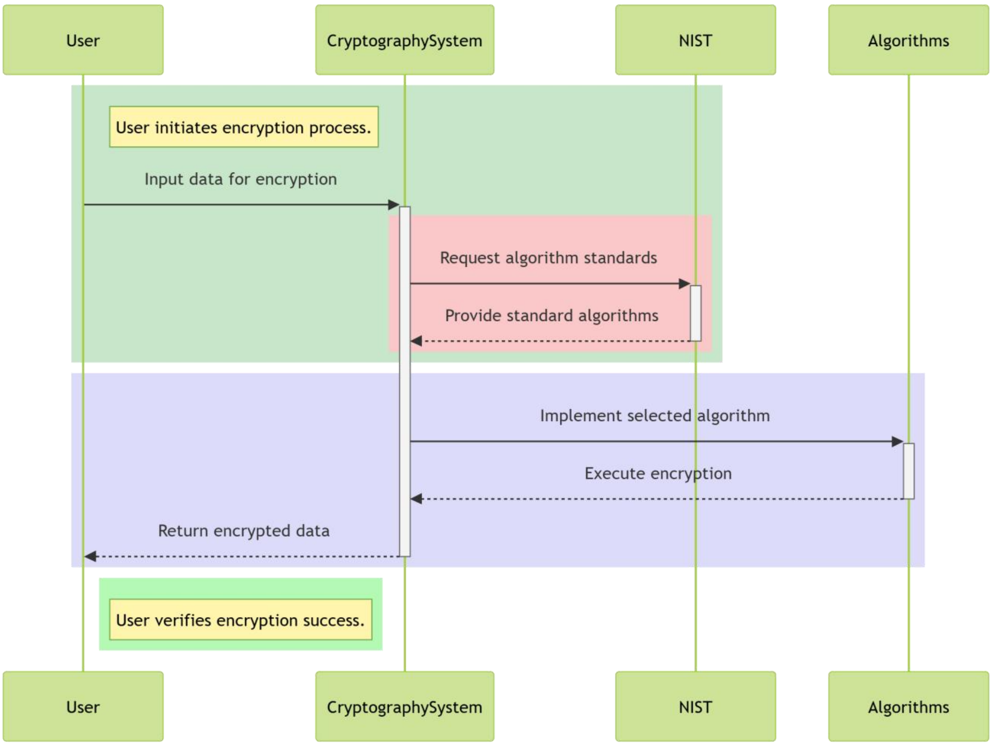
User
CryptographySystem
NIST
Algorithms
User initiates encryption process.
Input data for encryption
Request algorithm standards
Provide standard algorithms
Implement selected algorithm
Execute encryption
Return encrypted data
User verifies encryption success.
User
CryptographySystem
NIST
Algorithms

Figure 3: **The encryptions of data using modern cryptographic techniques.**

This ***Figure 3*** tells us how a user goes through the encryption process with the help of a cryptography system, leveraging standardized algorithms provided by NIST:

Starting the Encryption: The user decides they want to encrypt some data, so they initiate the process by sending that data to the **Cryptography System**.

Finding the Right Encryption Standards:

- The Cryptography System doesn't just use any random method; it reaches out to **NIST** (the National Institute of Standards and Technology), which is like the go-to authority for reliable encryption standards.
- NIST responds by sending back a set of approved algorithms that are secure and trustworthy.

Encrypting the Data:

- With NIST's standards in hand, the Cryptography System picks an appropriate encryption algorithm and starts the encryption process.
- It performs the encryption and securely encodes the user's data.

Returning the Encrypted Data: Once the encryption is done, the Cryptography System sends the encrypted data back to the user (Gilbert & Gilbert, 2024c).

User Verification: Finally, the user checks the encrypted data to ensure the process was successful.

The color-coding in the diagram shows the stages:

- **Green**: What the user does—starting the process and checking the outcome.
- **Red**: The Cryptography System's coordination with NIST to get the correct encryption standards.
- **Purple**: The actual encryption work, involving both the system and the selected algorithms.

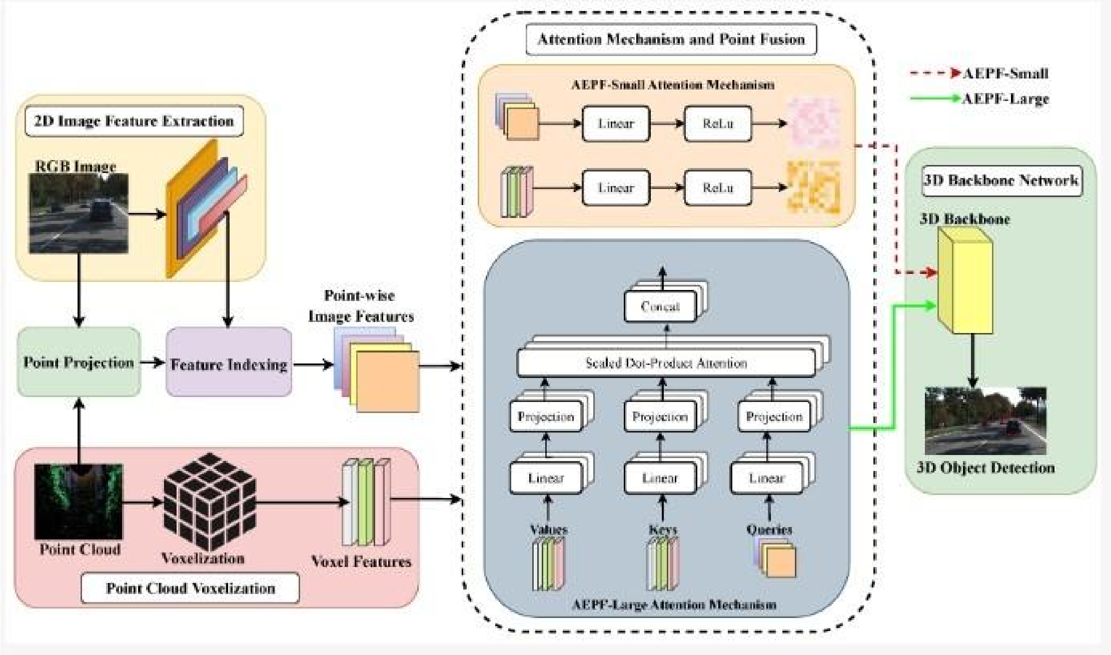

Figure 4: **Modern cryptography techniques** (Sharma, Meyer & Asher, 2024)

3. Fundamental Principles of Cryptography

Encryption plays a crucial role in securing the confidentiality and integrity of data by transforming information into a format that is only understandable by authorized entities (Saberi Kamarposhti, Ghorbani & Yadollahi, 2024; Gilbert & Gilbert, 2024d). Cryptographic hash functions are essential in preventing data tampering while it travels through insecure networks or when it is accessed by unauthorized internal parties. In cases where public key cryptography is insufficient, more robust cryptographic schemes are employed to further protect data (Sarkar, Chatterjee & Chakraborty, 2021). These schemes allow operations on encrypted data in a way that, when decrypted, the results are identical to what would have been achieved by directly working on the raw data, ensuring no advantage is gained by third-party adversaries. This process validates the integrity of the encrypted data before it is utilized (Zhang et al. 2018).

A study conducted during the COVID-19 pandemic examined the use of cryptography in securing personal health information and electronic health records (EHRs)(Koutsos et al.,2021). It provided a detailed comparison of necessary cryptographic approaches to ensure the secure operation of EHR systems and electronic ticketing systems. The research highlighted cryptographic techniques that met the security demands of integrated health diagnosis platforms and travel ticketing systems during the pandemic (Zhang et al. 2018; Gilbert & Gilbert, 2024f).

Cryptographic algorithms fall into two main categories: symmetric-key and asymmetric-key algorithms. Symmetric-key cryptography is typically used for secure data transmission, while asymmetric-key cryptography is more appropriate for digital signatures and key exchanges (Mohit, Kaur & Singh, 2024; Abilimi et al., 2015). Encryption guarantees the confidentiality of data, and asymmetric algorithms are generally better suited for key management because symmetric algorithms require a unique secret key for each communication pair. Key management practices are crucial, involving the dissemination and generation of numeric keys, especially in the context of RSA (Rivest Shamir Adleman) cryptography (Shah et al., 2023; Gilbert & Gilbert, 2024g). Additionally, secure protocols ensure that cryptographic algorithms are consistently applied correctly. Security systems need to be designed with both current and future threats in mind, as algorithms may eventually become vulnerable. Algorithmic agility, which allows for the replacement of compromised cryptography, is essential for maintaining long-term security (Gilbert & Gilbert, 2024i; Shah et al., 2023).

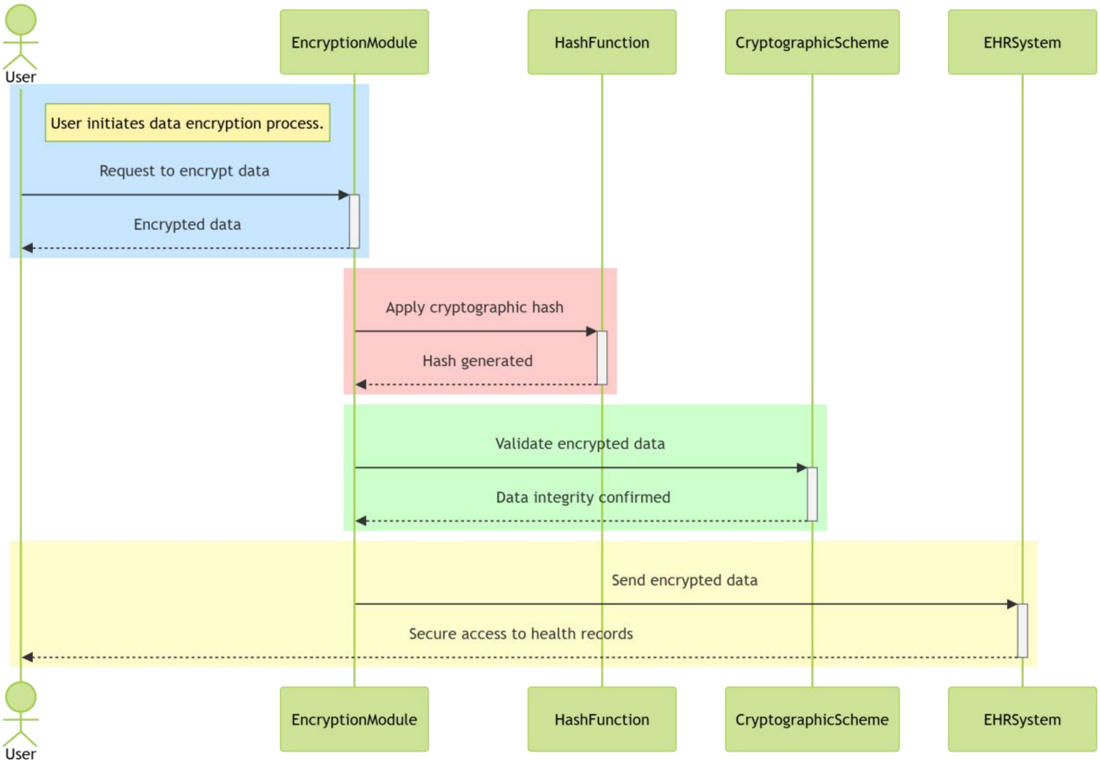

Figure 5: Data encryption safeguards confidentiality and integrity in systems.

Algorithms commonly associated with each principle are as follows:

1. Symmetric-key Encryption:

- AES (Advanced Encryption Standard): This is the gold standard for symmetric encryption. It's used in everything from securing websites to protecting sensitive government data. It has different key sizes (128, 192, 256 bits) for varying levels of security.
- DES (Data Encryption Standard): While largely considered outdated due to its relatively short key length, it was a foundational symmetric encryption algorithm.
- 3DES (Triple DES): An improvement on DES, applying the DES algorithm three times to each data block for increased security.
- Blowfish: A fast and efficient symmetric cipher, known for its variable key length.
- Twofish: A successor to Blowfish, designed to be even more secure and flexible.

2. Asymmetric-key Encryption:

- RSA (Rivest-Shamir-Adleman): A widely used algorithm for secure data transmission and digital signatures. It relies on the difficulty of factoring large numbers (Christopher, 2013).
- ECC (Elliptic Curve Cryptography): Offers similar security to RSA but with smaller key sizes, making it more efficient for mobile devices and other resource-constrained environments. ECDSA (Elliptic Curve Digital Signature Algorithm) is a common variant.

3. Cryptographic Hash Functions:

- SHA-1 (Secure Hash Algorithm 1): Once widely used, it's now considered less secure due to vulnerabilities.
- SHA-256/SHA-512: Members of the SHA-2 family, these are currently considered secure for most applications.
- MD5 (Message Digest Algorithm 5): Like SHA-1, it's no longer recommended for security-critical applications due to vulnerabilities.

4. Digital Signatures:

- RSA: Can be used for both encryption and digital signatures.
- ECDSA: Often preferred for digital signatures in modern applications due to its efficiency.

Important Considerations:

- Algorithm Agility: As mentioned in the text, it's crucial to be able to switch to newer, more secure algorithms as older ones become vulnerable.
- Key Management: The security of any cryptographic system depends heavily on proper key management. This includes secure generation, storage, and distribution of keys.
- Hybrid Approach: Many systems use a combination of symmetric and asymmetric cryptography. For example, asymmetric encryption might be used to securely exchange a symmetric key, which is then used for efficient encryption of large amounts of data (Gilbert & Gilbert, 2024k).

3.1. Confidentiality

Modern cryptography provides essential tools for ensuring crucial security needs, such as secure and confidential communications, digital signatures, and safe electronic transactions (Zeadally, Das & Sklavos, 2021). Its foundation lies in complex mathematical problems that are inherently difficult to solve, such as integer factorization and the discrete logarithm problem. The security of cryptographic systems is based on the fact that these problems are computationally infeasible to solve efficiently. However, this situation could change with the advent of quantum computers (QCs), which, with their immense computational power, could potentially solve these problems more efficiently (Wille et al., 2024; Gilbert & Gilbert, 2024j).

In August 1994, Piecuch introduced an innovative idea to strengthen the security of digital communication systems by incorporating a difficult signal recovery problem into the system's security mechanism(Shinde et al.,2024). In this system, two chaotic orbits from different chaos sources are generated and synchronized based on a scalar differential equation with a unidirectional drive-response coupling structure, influenced by an unknown gain(Lozi, 2023). Using a Lyapunov-like approach, the system provides sufficient conditions for the existence, uniqueness, and global exponential stability of a secure equilibrium point. The signal recovery method is impracticable under general conditions, offering strong security(Belhadjoudja, 2021).

A numerical example of chaos synchronization in a selected secure drive-response mode demonstrates the system's robustness. The phase-type secure communication system, which leverages Niewolne nonlinearity, proves effective in securely transmitting short encrypted messages. The overwhelming complexity involved in identifying the drive-response relationship ensures that the digital communication system remains nearly impervious to traditional cryptanalysis techniques (Belhadjoudja, 2021; Gilbert & Gilbert, 2024l).See figure below:

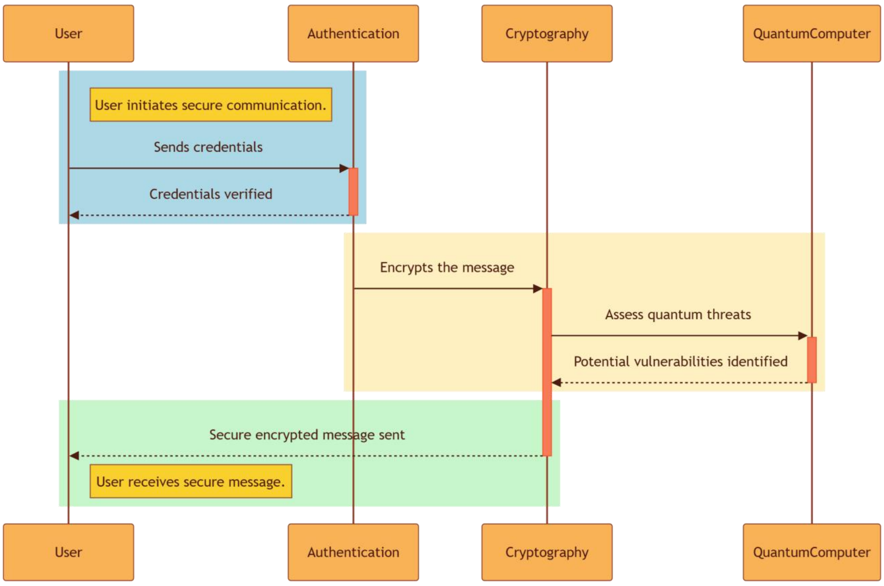

Figure 6: Secure communication utilizing cryptography and quantum threats.

3.2. Integrity

This algorithm, while nonlinear, differs from traditional Feedback Control Systems (FCS) (Belhadjoudja, 2021; Gilbert & Gilbert, 2024m) in that the observer can estimate the state of unobservable one-way interactions and synchronize systems of the same order without constraints on that order. A complete characterization of the observer law guarantees the ability to estimate the state vector of a dynamic host system. This approach ensures that data remains secure and untampered during transmission(Alquwayzani & Albuali, 2024). Additionally, it resolves the challenge of transmitting dynamic monitoring data from a fog node in a decentralized fog environment, while reducing bandwidth and storage overhead in the ciphertext transmission process(Agrawal, Singhal & Sharma, 2024). Even if cloud or fog nodes are malicious or unauthorized, this scheme prevents them from reading attribute information, message content, or making unauthorized dynamic updates. In modern industrial cryptographic systems, symmetric encryption is typically employed for encryption, while digital signatures are used for message integrity and non-repudiation (Zang et al., 2021). A cryptographic algorithm is deemed "secure" when data destruction is irreversible—this is known as "preimage resistance," "message integrity," or "non-repudiation"(Gilbert, 2018; Mago, 2016). The articles in the current Special Issue introduce new cryptographic algorithms, one for streaming data and two others for enhancing encryption processing efficiency with large datasets (Thabit et al.,2023).See figure below

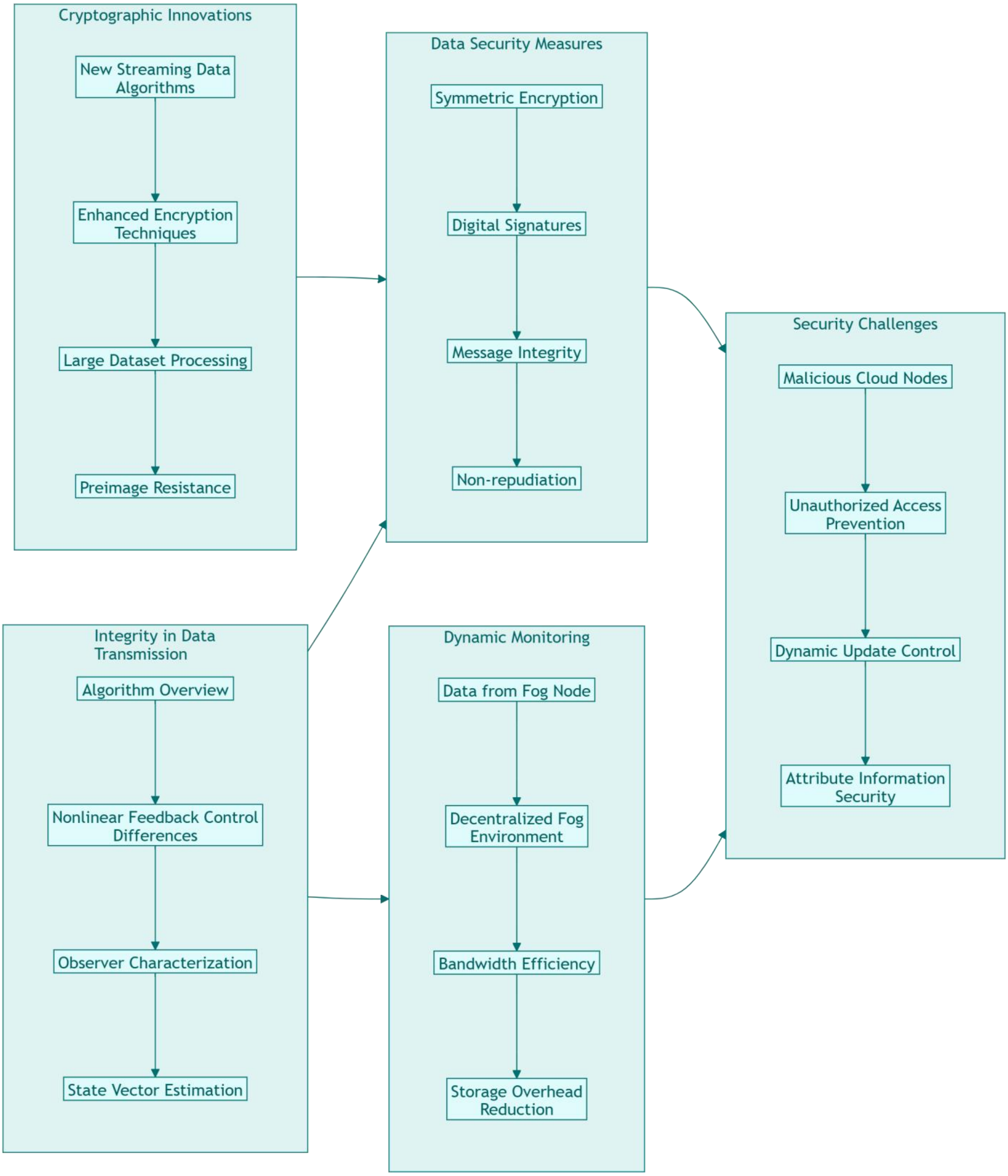

Figure 7: Integrity ensures secure data transmission and system synchronization.

3.3. Authentication

Authentication and digital signatures are fundamentally tied to the accuracy and reliability of public key infrastructure (PKI)(Danquah & Kwabena-Adade, 2020). Digital signatures play a key role in ensuring data integrity and preventing unauthorized modifications. For secure key distribution, hybrid cryptosystems are often used, where documents are split into separate parts for distribution across a network. In public auditable cloud data auditing protocols, secure collaboration is essential between data owners and auditors, although the process can suffer from significant e-signature overhead, reducing overall efficiency (Huang et al.,2020).

Cryptographic systems maintain message integrity by embedding hash values and employing password-authenticated hashing techniques (Das, Hesse & Lehmann, 2022; Gilbert & Gilbert, 2024n). The results indicate that these systems provide strong encryption, ensuring both data privacy and integrity. Research has explored the integrity and authenticity elements of signature schemes, leading to the identification of various generic attacks. While quantum computers pose a threat to cryptographic primitives like RSA and other public key cryptography methods, certain symmetric-key algorithms are expected to remain secure despite advances in quantum computing (Tom et al., 2023; Gilbert & Gilbert, 2024j).See figure below:

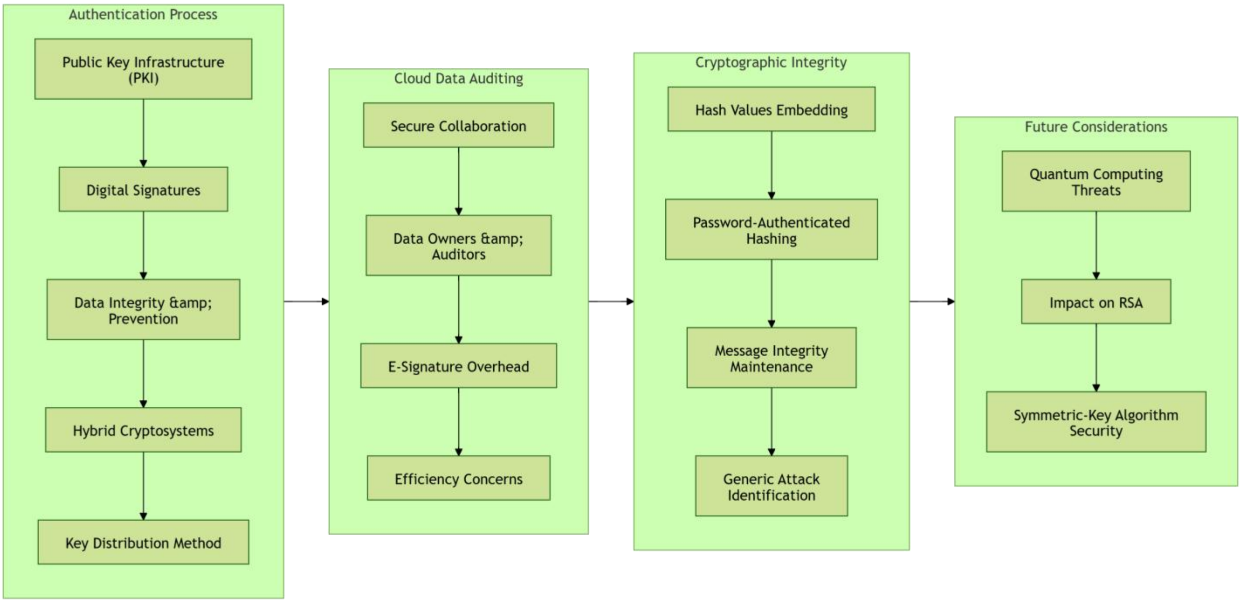

Figure 8: This diagram illustrates the authentication process steps.

3.4. Non-Repudiation

In this section, we explore existing models for non-repudiation and categorize the various non-repudiation protocols based on the authentication methods used for verification and the involvement of third parties (Chen et al., 2022). One model is abstract, where a pair of digital signatures may be challenging to compare, raising questions like whether a signer has been impersonated(Müller et al.,2019). The process of verifying the sender begins with having the signer commit to a specific action, with their signature and a symmetric key provided by the verifier (Lara et al.,2019). This method is considered a non-interactive authenticated key establishment protocol. Session keys are established interactively, often based on the verifier's assumptions regarding the forger(Arun, Bonneau & Clark, 2022). We also provide a model for experimental security, particularly focusing on key establishment using email-like models without common channel assumptions, linking keys to atomic formulas (Tsipenyuk, 2018). In our key establishment results, we outline the infeasibility of certain generic protocols, which may seem straightforward from a structured perspective.

Signature and non-repudiation systems are becoming increasingly important, especially in financial and governmental services. These systems allow a sender to bind themselves to a message, enabling anyone to verify the origin of the signature ((Banerjee & Saha, 2024)). Furthermore, two critical properties of signatures include that the signer cannot dissociate themselves from the message, ensuring that the signature remains valid. The security of such systems is usually based on assumptions that are difficult to solve, such as the discrete logarithm problem or factoring large numbers. Zero-knowledge proofs are a key cryptographic concept used to demonstrate the security and soundness of commitment schemes, which are later used to secure cryptographic protocols (Gilbert & Gilbert, 2024i). Additionally, we provide examples of commitments and suggest ways they can be utilized to build secure signature systems. Non-repudiation can be defined as the act of digitally signing a message using an asymmetric cryptographic scheme, in such a way that the signature can be verified using the public key, and the signer cannot deny having signed the message (Banerjee & Saha, 2024; Gilbert & Gilbert, 2024f). See figure below:

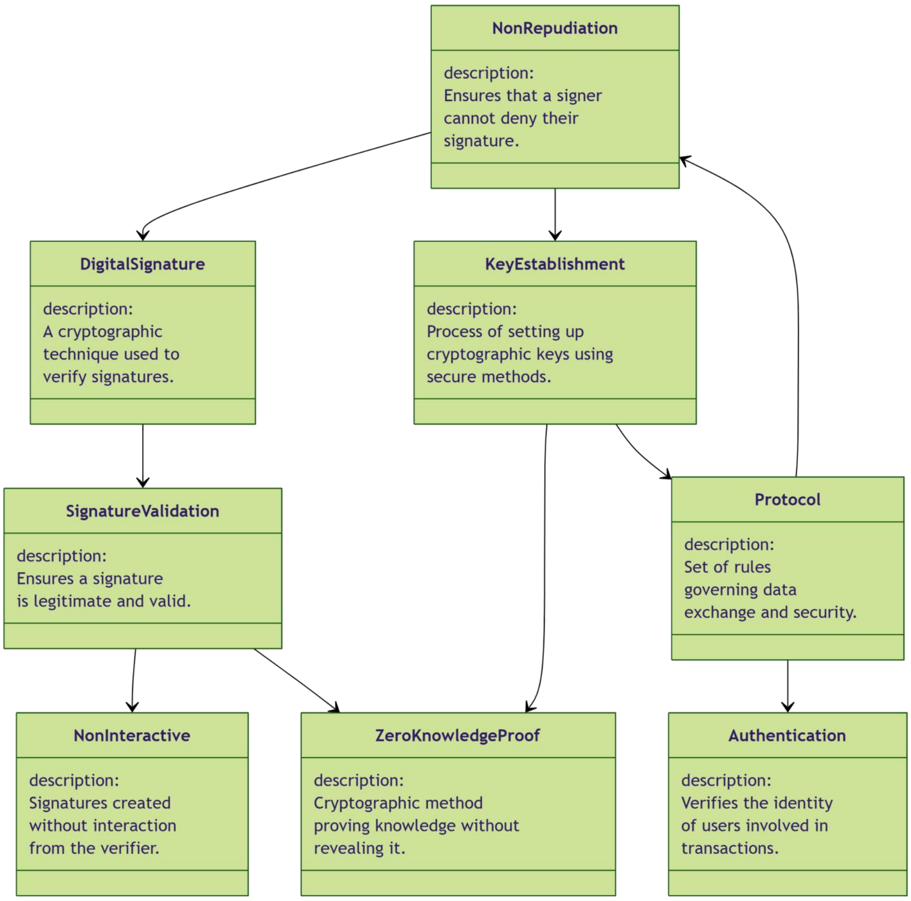

Figure 9: Models non-repudiation protocols and their components.

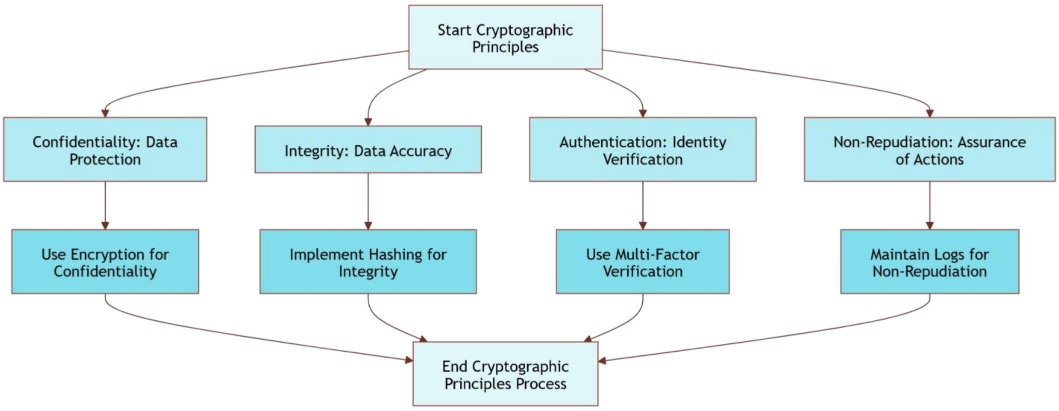
Start Cryptographic Principles
Confidentiality: Data Protection
Integrity: Data Accuracy
Authentication: Identity Verification
Non-Repudiation: Assurance of Actions
Use Encryption for Confidentiality
Implement Hashing for Integrity
Use Multi-Factor Verification
Maintain Logs for Non-Repudiation
End Cryptographic Principles Process

Figure 10: Confidentiality, Integrity, authentication, and repudiation for system synchronization.

This diagram breaks down four essential principles of cryptography, showing how they work together to keep our data safe and trustworthy:

- **Confidentiality**: Think of this as the "privacy shield" for information. It's all about keeping data hidden from prying eyes. Encryption is the main tool here—like locking sensitive information in a digital safe that only authorized people have the key to. This way, if data is intercepted, it remains unreadable and secure.
- **Integrity**: This ensures that data stays true and unaltered from the time it's created to the time it's used. Imagine it as a digital "seal of authenticity." Hashing, a kind of digital fingerprint, helps detect if even the tiniest change is made to the data, so we can be sure it hasn't been tampered with.
- **Authentication**: This is the "ID check" of cryptography, making sure people are who they say they are before granting access. Multi-factor authentication, like combining a password with a fingerprint, adds layers of verification so only the right person can access sensitive information.

- **Non-Repudiation**: This principle is about "accountability." It ensures that once someone takes an action, like sending a message or signing a document, they can't deny doing it. By keeping logs of actions, we create a record of who did what, which helps maintain trust and accountability.

The summary of the algorithms for the principles are as follows:

Confidentiality: Keep the Data Private

1. Goal: Make sure only authorized people can see the data.
2. How: Lock up the data using encryption. Imagine turning it into a secret code that only someone with the right key can unlock.
3. What You Do: Use an encryption method like AES or RSA to scramble the data before sending or storing it.

Integrity: Keep the Data Honest

1. Goal: Ensure the data hasn't been tampered with.
2. How: Create a "digital fingerprint" of the data using a hashing function. This fingerprint is unique to the original data.
3. What You Do: Run the data through a hashing algorithm (like SHA-256). Save the result as a reference. Later, if you want to check that the data is still intact, just re-hash it and compare fingerprints. If they match, the data is authentic.

Authentication: Verify Who's Accessing the Data

1. Goal: Confirm that the person trying to access the data is who they claim to be.
2. How: Use multi-factor authentication, like a password plus a fingerprint scan, to make it harder for intruders to gain access.
3. What You Do: Request the user's credentials, which could be something they know (like a password) or something they have (like a phone for a code). If their credentials are verified, grant access. If not, block access and keep a record of the attempt.

Non-Repudiation: Keep a Record of Actions

1. Goal: Make sure users can't deny their actions within the system later.
2. How: Log actions, like a digital paper trail that shows who did what and when.
3. What You Do: Every time a user performs an important action (like approving a transaction), record it along with their identity and a timestamp. Sign this record so it can't be changed. This way, you have proof if they later deny their involvement.

4. Key Cryptographic Algorithms

The RSA (Rivest, Shamir, and Adleman) algorithm is recommended by NIST for securing information systems through encryption and signature generation (Christopher, 2013; Mpitsi, 2024). The security of RSA is based on the computational difficulty of factoring the product of two large prime numbers. The secret key, used for encryption, is a pair (d, n), and the algorithm can be implemented with key sizes starting at 1024 bits(Imam et al.,2021). At this size, RSA is considered secure, but the security level depends on the length of the key.

Elliptic Curve Cryptography (ECC) is another form of asymmetric cryptography that operates differently from RSA(Al-Shabi, 2019). ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem, where finding k in the equation x = Pk is computationally infeasible when P and x are known. Compared to RSA, ECC offers shorter key lengths for the same level of security—ECC-164 provides the same security as RSA-1024. Elliptic curves are highly efficient in public key cryptography applications, such as digital signatures and key exchange protocols (Mahto & Yadav, 2017). Due to their efficiency in speed, resource consumption, and security, elliptic curves have become the focus of cryptanalysts proposing improved recommendations for digital signatures, public key encryption, and key exchange protocols.

Encryption is one of the central concepts in cryptography, converting plaintext into ciphertext to protect data during transmission or storage(Seth et al.,2022). Cryptographic algorithms must be computationally secure, meaning they should have a sufficiently large key space and be executable within a reasonable time frame. The Advanced Encryption Standard (AES) family is a widely used symmetric encryption algorithm. AES operates as a block cipher, encrypting fixed-size blocks of data. The strength of AES is determined by the key length, which comes in three standard sizes: AES-128, AES-192, and AES-256(Thaenkaew, Quoitin & Meddahi, 2023) (Bhowmik & Menon, 2021). Currently, the only feasible attack against AES is a brute-force attack, which would require 2^127 operations to succeed. The best bound for attacks against AES-192 is approximately 1536 operations, derived from the multiplication of the maximum bit block length and the maximum number of operations calculated against 512(van de Graaf & Lenstra, 2024).

4.1. RSA Algorithm

To date, there has been no standardized method for building secure communication systems capable of withstanding adversaries who utilize sub-exponential or quantum algorithms. The core problem of RSA encryption, known as the factorization problem, can potentially be solved by an adversary using a quantum computer, as this problem belongs to a class of mathematical problems that can be reduced to Shor's polynomial time algorithm, O(2^n)(Tom et al.,2023). However, elliptic curve cryptography (ECC) operates on entirely different mathematical principles than the factorization problem, so while the classical public key cryptosystems like RSA may be vulnerable to quantum computing, ECC may offer a more resilient option. As we approach the quantum era, cryptographic development is increasingly focused on protecting resources and addressing the future challenges posed by quantum computing(Sahu & Mazumdar, 2024). Addressing this issue requires significant effort from young and talented individuals, as the future of cryptographic security will depend on their contributions.

This section examines the evolution of cryptographic algorithms, specifically the RSA algorithm, in response to the growing threat of cyberattacks. It explores public key cryptography, the steps involved in the RSA algorithm, why it is considered secure, and the challenges it faces in the future. The development of RSA encryption has resolved the long-standing issue of key distribution in information security by leveraging public key cryptography(Gour et al.,2024). RSA's security is based on the immense computational difficulty involved in factoring very large numbers. The algorithm is built on three key structures: modular exponentiation, modular division, and a reversible process. RSA remains secure due to the significant computational challenge of factoring large numbers(Singh et al.,2024). Specifically, the use of prime numbers to achieve modular decomposition increases the complexity of factoring large numbers, ensuring that RSA encryption will remain secure as long as the moduli contain two large prime numbers.

4.2. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) relies on a one-way mathematical function. Here's an example of how ECC works in the context of digital signatures. Imagine Alice wants to send a message to Bob and sign it digitally using ECC. To do this, Alice needs to generate a pair of private and public keys using ECC. She selects a secret number, known as her private key, and a point on the elliptic curve, called the "secret point." This secret point is then multiplied by a predefined value, resulting in a new point on the curve. Next, Alice hashes the message along with her keys to generate a hash value, which she uses to sign the message. Bob, using Alice's public key, can verify the message by computing the hash and checking if it matches. If the two hash values align, it confirms that Alice is the sender of the message (Al-Zubaidie, Zhang & Zhang, 2019).

As noted by Ullah et al.(2023), unlike RSA and DSA, which involve multiplying or raising numbers to generate keys, ECC uses points on a graph. This method of key generation provides a higher level of security because retrieving the private key from the public key would require reconstructing the entire elliptic curve, which is computationally infeasible(Hagras et al.,2023). ECC also has the advantage of generating much smaller keys compared to RSA, while still offering the same level of security(Imam et al.,2021). As more connected devices emerge, the importance of ECC grows, especially in resource-constrained environments. ECC is standardized in several protocols, including IEEE 1363-2000, IEEE Std 1363a-2004, and IEEE Std 1363-2000(Sabbry & Levina, 2024).

4.3. Advanced Encryption Standard (AES)

Various techniques have been developed to protect electronic assets such as photos, documents, and audio-visual communications without compromising their integrity or confidentiality. With the widespread use of the internet, ensuring privacy during communication has become a fundamental need. In response, three primary types of cryptographic techniques have emerged to safeguard the transmission of electronic data online: symmetric encryption, asymmetric encryption, and hash functions (Gilbert & Gilbert, 2024h). Symmetric encryption involves using the same key for both encryption and decryption, whereas asymmetric encryption utilizes a pair of keys—one for encryption and another for decryption (Halak, Yilmaz & Shiu, 2022). The security of these methods depends heavily on the confidentiality of the keys. Public key encryption, for example, assigns a private key and a corresponding public key to each user. Initially, DES (Data Encryption Standard) was widely considered the go-to encryption method for official and commercial applications (e.g., UNIX, Windows) (Gilbert & Gilbert, 2024m). However, DES began to show vulnerabilities, particularly as cryptographic keys could be discovered and exploited, as noted by Horst Feistel. As a result, alternatives like LOKI89 and FEAL were developed, but they, too, were found insufficient as long-term solutions (Gilbert & Gilbert, 2024k).

The Advanced Encryption Standard (AES) was introduced in 2001 by the National Institute of Standards and Technology (NIST) to replace DES, which had become weak due to its 56-bit key length, making it vulnerable to brute-force attacks (Umay, 2024). AES, with key lengths of 128, 192, and 256 bits, offers far greater security. For instance, while it took an estimated five days in the 1990s to find a DES key using brute-force techniques on an average computer, cracking an AES-128 key would take billions of years. In essence, AES divides input data into blocks and performs simple bit-shuffling operations, resulting in ciphered blocks of data. These operations shuffle the bits in ways that are not easily distinguishable, making brute-force attacks highly impractical (Sarkar et al., 2024). Even if attackers attempt to model the shuffling processes, the complex and randomized operations of AES make it extremely difficult to decrypt without the proper key.

5. Strengths and Weaknesses of Cryptographic Algorithms

Cryptographic algorithms can be mathematically defined, and they generally have two main criteria that determine their effectiveness: strengths and weaknesses. The strength of a cryptographic algorithm is often gauged by how fast it can perform encryption and decryption while maintaining security. A robust and efficient cryptographic algorithm is one that is harder to break due to its complexity (Abood & Guirguis, 2018). For encryption and decryption to remain secure, users may need to compromise on processing speed. This is especially true in symmetric cryptographic systems, which are generally more versatile. One of the earliest examples of such a system is the Enigma machine, designed to secure communications during wartime(Marks, 2024). However, the history of cryptography demonstrates that no system is invulnerable—eventually, even the most secure systems have been broken by experts.

This article provides an in-depth discussion on the origins, purposes, and properties of cryptographic algorithms, with particular focus on how these algorithms have evolved to address emerging threats (Thabit et al., 2023; Gilbert & Gilbert, 2024k). The paper explores the strengths and vulnerabilities of cryptographic systems, emphasizing the balance between security and performance. Additionally, it examines the specific conditions necessary for cryptographic algorithms to function securely, touching on the inherent weaknesses of both symmetric and asymmetric encryption techniques (Frank, 2024). The article also highlights the importance of ensuring proper authentication protocols for various components of communication systems, including network devices (Rao & Deebak, 2023).

5.1. RSA Algorithm

Many public key cryptosystems rely heavily on operations involving large numbers. For instance, the RSA algorithm, which is widely used in commercial applications, typically employs key lengths of up to 2048 bits (Anwar et al.,2019). This has made RSA one of the most commonly used public key cryptosystems in practical applications. However, the security of RSA is contingent upon the difficulty of factoring large numbers. If a method is found to efficiently factor these large numbers, the security of RSA will be compromised. Thus, RSA's security is fundamentally tied to the challenge of determining the prime factors of a composite number. As advancements in quantum computing progress, especially in areas such as quantum cryptanalysis, RSA may face new vulnerabilities that necessitate improvements(Sahu & Mazumdar, 2024).

The RSA algorithm works by utilizing two large prime numbers, ppp and qqq, to generate a public encryption key (n,e)(n, e)(n,e) and a private decryption key ddd (Lavanya, 2018). Its security relies on the assumption that factoring nnn, which is the product of ppp and qqq, is computationally infeasible. In related research, other cryptosystems, such as NTRU, rely on different mathematical structures, like finding the shortest vectors in ideal lattices ((Albrecht & Ducas, 2021). However, weaknesses have been identified in various cryptosystems. For example, if the problem is easily solvable by an unproven quantum computer, such as in the case of the NTRU cryptosystem, the security can be compromised. Additionally, RSA's reliance on factoring two large prime numbers presents a vulnerability to quantum attacks.

These potential vulnerabilities underscore the urgent need to develop quantum-resistant cryptosystems. One solution is to further explore and strengthen the RSA algorithm to withstand quantum computer attacks (Ajala,2024). Another approach involves studying quantum algorithms, such as Shor's and Grover's algorithms, to understand how quantum principles could affect cryptographic security and develop strategies to mitigate these risks.

5.2. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) has gained significant popularity in public key cryptography (PKC) due to its broad range of applications, including data encryption for confidentiality and digital signatures for integrity in resource-constrained environments like RFID, supply chain management, smartphones, and the Internet of Things (Ullah,2023). One of the primary advantages of ECC is its requirement for shorter key lengths, reduced bandwidth, and lower computational power compared to traditional public key cryptography methods like RSA and DSA(Alhaj, Alrabea & Jawabreh, 2024). This efficiency has made ECC highly suitable for applications where performance and cost are critical factors. For example, the Moversense sensor, alongside the OpenSSL 'ec' command, has successfully adopted ECC for ensuring the privacy of remote patient monitoring systems (Suárez-Albela et al., 2018; Gilbert & Gilbert, 2024i). Despite technological advancements, achieving similar security and performance properties across various systems remains challenging. However, ECC's unique mathematical properties, such as its elliptic curve topologies, provide robust security while being less sensitive to changes in parameters like cardinality in elliptic curves, which makes it well-suited for post-quantum secure intrusion and wireless secret communication systems.

ECC operates using elliptic curve group operations and is regarded as one of the most efficient cryptographic algorithms, especially when compared to other public-key algorithms. One of its key strengths lies in the fact that ECC requires much smaller key sizes—approximately 16 times smaller than those required by RSA (Al-Zubaidie, Zhang & Zhang, 2019). This smaller key size allows ECC to maintain high security while minimizing the computational resources needed, making it ideal for big data applications and other similar uses. Additionally, while both ECC and RSA use different mathematical structures for their cryptographic processes, it is generally easier and more efficient to design processors for RSA than for ECC due to their distinct mathematical frameworks. Nevertheless, ECC's superior performance in constrained environments makes it an essential tool in modern cryptography.

5.3. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) involves several field operations depending on the key length (Abdullah, 2017). For instance, 128-bit keys require 12 operations per round, while 192- and 256-bit keys require 14 operations per round. Each column in the encryption process operates independently but is later mixed. The number of SK mode changes is adjusted by a factor of 4. During the process, the speeds in multiple lines are optimized at the conclusion of the confusion cycle. Following the MixColumns operation, the K value is renewed, and the next cycle of operations continues. The number of rounds is adjusted according to the security levels required for each key length, which is set when the key is first generated (Kumar et al.,2021).

The Secure Hash Algorithm (SHA-2) family, which emphasizes collision resistance, was submitted to the National Institute of Standards and Technology (NIST) as part of the SHA-3 competition. In the encryption process, four critical steps are executed: State, Key-whitening, SubBytes, and MixColumns operations(Tolba, 2024). Each round begins by randomly creating a 4 × 4 column of bytes. This initial step, called SubBytes, is followed by ShiftRows, which removes any discrepancies between the state and the encryption key. The third step involves mixing the columns, and finally, KeyWhitening is performed as the last step in every round (Shabbir et al, 2019).

In response to the growing demand for robust cryptographic algorithms, NIST issued a public call for submissions in 1997 to establish a new cryptographic standard. This call resulted in the selection of AES from 15 candidate algorithms. The proposed routing algorithms included well-known options such as RSA, CAST, Mars, RC6, Rijndael, Serpent, and Twofish (Wollinger, Guajardo & Paar, 2004; Awan et al.,2020). AES emerged as the standard from this selection process due to its ability to meet modern security requirements for information and communication technology. The chosen AES algorithm supports key lengths of 128, 192, and 256 bits, employing both communication rounds and diffusion rounds to ensure secure encryption and decryption processes. The various changes in the diffusion cycle were designed to enhance the overall security and effectiveness of the algorithm.

6. Cryptographic Attacks and Countermeasures

Achieving perfect security, meaning a system invulnerable to any type of attack, remains an impossible goal. Cyber-attacks, particularly those involving malicious software, are among the most serious threats in the realm of computer security(Mallick & Nath, 2024). Even with protective measures in place, systems must continually evolve to counter newly developed cryptographic attacks. This review aims to present various methods for detecting attacks on cryptographic systems, analyzing characteristics of cyber zero-day attack datasets based on specific features and types. The study also evaluates the effectiveness and limitations of state-of-the-art machine learning algorithms for detecting cyber-attacks in mobile networks (Khaleel et al., 2024; Gilbert, Oluwatosin & Gilbert, 2024; Yeboah & Abilimi, 2013).

Cryptographic attacks generally target the recovery of keys, plaintext messages, or other sensitive information hidden within the ciphertext (Mohamed & Mohamed, 2020). These attacks bypass the algorithm’s security mechanisms without directly attacking the cryptographic algorithm itself (Mousavi et al., 2021). Cryptanalysis techniques, which rely on analyzing publicly available information, are considered more dangerous than brute-force attacks. While brute force involves blindly attempting to guess a key, cryptanalysis can identify vulnerabilities within an algorithm, making it easier to extract the secret data. Given the significant rise in cyber-attacks and security breaches in recent years, computers connected to networks without adequate protection are easy targets for hackers, who can spy on or damage the system's contents without the user's knowledge (Aslan et al., 2023).

6.1. Brute Force Attacks

To effectively prevent brute-force attacks, a cryptographic key should be long, randomly generated, and uniquely distinctive. Industry standards recommend that such keys have a minimum length of 128 bits to ensure a high level of security(Gebremichael et al., 2020). The strength of these keys is often measured through metrics like Hamming Weight and Entropy. Entropy, in the context of computer security, quantifies the randomness in a key—measured in bits. The greater the entropy, the more random the key, thus reducing the likelihood of success for brute-force attacks (Hasan et al.,2023). As the saying goes, "Chance favors the prepared mind"—in this case, a key with high entropy is well-prepared to thwart potential threats.

However, when an encryption key has structural weaknesses, such as repetitive byte patterns, attackers can use these patterns to deduce parameters and crack the encryption. Symmetric cryptographic systems, which use the same key for both encryption and decryption, are particularly vulnerable if such weaknesses exist(Alenezi, Alabdulrazzaq & Mohammad, 2020). In comparison to more robust encryption systems, weak symmetric cryptography is far easier to break(Aumasson, 2024).

Symmetric encryption involves using the same key, or a key pair, for both encryption and decryption. Block and stream ciphers are widely used in symmetric algorithms(Alenezi, Alabdulrazzaq & Mohammad, 2020). The vulnerability of symmetric encryption lies in the limited number of possible keys, making them susceptible to brute-force attacks. In this method, an attacker systematically attempts every possible key until the correct one is found, exploiting the finite nature of the key space. As in the movie *The Imitation Game*, where Alan Turing emphasizes, "Sometimes it is the very people who no one imagines anything of who do the things that no one can imagine"—even in cryptography, unanticipated patterns can sometimes be the very weakness that makes the system vulnerable (WARSONO, 2016).

6.2. Side-Channel Attacks

Recent studies aimed at enhancing the security of embedded devices have identified side-channel attacks as a significant risk. These attacks target exposed interfaces that can exploit cryptographic implementations within embedded sensor systems. It's crucial to understand that these attacks often rely on passive observation, meaning no direct manipulation of the system occurs. Instead, they can extract sensitive data used in cryptographic operations, such as keys, input ciphertexts, or even implementation details, like the dominant computing unit in use. It's important to note that not all cryptographic systems are equally susceptible to these attacks, as vulnerabilities vary based on the system design and implementation (Santoso & Oohama, 2019).

The core objective in defending cryptographic implementations against side-channel attacks is to prevent malicious actors from accessing sensitive data through passive means. In the context of embedded sensor systems, particularly those used in the rapidly growing field of digital healthcare, securing communication between sensors, edge devices, and databases has become essential. The increase in digital health services has heightened the demand for robust security measures to safeguard data and system integrity (Santoso & Oohama, 2019).

Side-channel attacks represent a serious threat to secure systems, as they can reveal sensitive information such as cryptographic keys through various forms of analysis—timing, power consumption, electromagnetic emissions, or even acoustic signals(Sayakkara, Le-Khac & Scanlon, 2019). With cryptographic implementations becoming cheaper and more integrated, the risk of insecure hardware increases (Singh et al.,2024). While both researchers and industry professionals have explored ways to fortify cryptographic systems against these physical threats, a comprehensive, scalable measurement of how cryptographic computations correlate with externally observable factors—particularly in the context of embedded devices like smart healthcare systems—remains underdeveloped. Numerous hardware-based attacks, such as Side-Channel Attacks (SCA), are known and remain highly effective in practice (Mushtaq et al.,2020).

6.3. Quantum Cryptanalysis

This paper introduces new classes of signature schemes and public key encryption schemes, where the security relies on the quantum resistance of cryptographic hash functions. The first class of primitives, known as pOSEs (**post-quantum One-time Signature schemes with Encryption**), uses a universal one-time pad for authenticated encryption. Another approach for achieving quantum-secure signatures involves the use of quantum-secure pseudo-random functions or permutations(Ciulei, Crețu & Simion, 2022). Additionally, public key encryption schemes and related constructions for encryption have been discussed in quantum literature, specifically in the context of quantum-secure QROM computations (Babu et al.,2024). These constructions have been demonstrated to be secure against QROM adversaries when quantum-accessible random oracles are involved. However, no practical query models for encryption targeting immortal adversaries have been thoroughly examined in post-quantum security schemes.

Despite ongoing efforts over the past few decades to develop quantum-resistant cryptographic schemes, researchers continue to uncover new large-scale quantum algorithms that pose a threat to these cryptographic solutions (Andronikos & Sirokofskich, 2023; Zunaidi, Sayakkara & Scanlon, 2024). For example, new families of concrete polynomial-time quantum-secure hash functions with a high probability of collision have been discovered, although no effective quantum algorithms have yet been identified to distinguish them (Suhail et al.,2020). Despite the growing arsenal of quantum cryptographic attacks, many families of hash functions, such as those based on the Merkle-Damgård construction, cannot be made quantum-secure. Therefore, it is recommended to phase out these older hash functions and replace them with ones designed specifically for quantum security(Algazy et al., 2024).

7. Current Trends in Cryptographic Research

As computational technology continues to evolve, the methods required to safeguard modern electronic communication must also adapt. One of the most heavily researched—though still largely theoretical—developments is quantum computing. Quantum computers are expected to solve problems that are currently impossible for conventional technology to handle within a reasonable time frame (De Leon et al.,2021). Since cryptography relies on the difficulty of solving certain problems (such as ensuring that encryption cannot be broken without an impractically high computational effort), the potential of quantum computing poses significant implications for long-term security (SaberiKamarposhti, Ghorbani & Yadollahi, 2024). As a result, the development of cryptographic primitives that can withstand quantum-based algorithms has become an active area of research.

In the near term, however, other pressing concerns also demand attention. The growing computational power of classical computers means that cryptographic systems must continue to resist these advances(Tom et al., 2023). Although current protocols and algorithms are believed to be secure, the increasing capability of potential adversaries will intensify the challenge of maintaining this security. This creates a continuous race between those seeking to enhance cryptographic protection and those attempting to overcome it.

Cryptography has safeguarded private communications for centuries, and over the past 150 years, advancements in cryptographic science have paralleled increases in computational power (Kumar et al., 2021). However, the rapid growth of computing in recent decades has significantly broadened the scope of what must be protected by cryptographic means. As modern cryptographic systems evolve to meet these demands, research has encountered several challenges that must be addressed to ensure future security. This paper offers an overview of current trends in cryptographic research and suggests areas of focus for the future.

7.1. Post-Quantum Cryptography

New cryptographic algorithms designed to be resistant to quantum computing threats, known as post-quantum cryptographic algorithms, aim to remain effective in the era of quantum computers. These algorithms are developed using various advanced technologies. Several proposals focus on creating a public key factory algorithm based on lattice algorithms, whether they employ a module in a ring, a vector space, or other structures. Among these, lattice-based cryptosystems are currently the most advanced in the realm of post-quantum cryptography. A key quantum threat is the quantum factorization algorithm, which can efficiently factor large integers—a process critical to the security of many current cryptographic systems. This could have severe consequences for the online security of transaction systems, as classical systems may be unable to respond swiftly enough. Authentication of messages can be achieved with the ECIES algorithm, ECDSA, or elliptic curve digital signature algorithms, all of which rely on operations involving the public and private keys of the sender and receiver to verify the authenticity of a message.

Although quantum computers are not yet fully reliable, their potential to break existing cryptographic algorithms, particularly those involving public keys, presents a significant threat to the security of networks and data. This highlights the growing necessity for post-quantum cryptography (Kumar et al., 2021). Three possible future scenarios exist: quantum computers may never be built to a scale that poses a threat, they may never be able to solve problems like integer factorization or discrete logarithms, or we may successfully establish quantum-resistant cryptosystems before they emerge. At the very least, it is prudent to begin experimenting with potential solutions now ((Bavdekar et al.,2022). While no current quantum computer has solved the integer factorization and discrete logarithm problems using Shor's algorithm, research on quantum algorithms continues to progress. Therefore, this issue warrants attention (Bansod & Ragha, 2022).

7.2. Homomorphic Encryption

Homomorphic encryption can be understood through a metaphor often used to explain the differences between encryption schemes. Imagine a secure room where computations are performed. In a somewhat homomorphic encryption scheme, the room may not be fully secure, but there's an armored glass window that allows someone to see the encrypted output of whatever is happening inside without revealing any sensitive details. In contrast, in a partially homomorphic encryption scheme, the entire room is secure and opaque—no one can see what's inside, but computations are limited to either addition or multiplication, not both (Acar et al.,2018).

Homomorphic encryption is a type of encryption that permits computations on encrypted data (ciphertext) while maintaining security. When the encrypted result is decrypted, it matches the outcome as if the operations were carried out on the plaintext data itself (Jiang et al.,2019). This capability has diverse applications, including voting systems, data aggregation, and searchable encryption systems. However, fully homomorphic encryption—allowing both addition and multiplication—is currently impractical due to its computational complexity (Acar et al.,2018). As a result, only "somewhat" and "partially" homomorphic encryption schemes are widely used today.

7.3. Blockchain and Cryptography

Blockchains are increasingly being viewed as an ideal back-end technology for the Internet of Things (IoT) (Gilbert & Gilbert, 2024e). They decentralize trust among participants and offer important features such as transparency, auditability, organized data storage, and the ability to revalidate data over long periods of time (Acar et al., 2018; Gilbert & Gilbert, 2024h). A key consideration for the development of IoT applications using blockchain technology is the incorporation of Quantum Key Distribution (QKD)(Gilbert & Gilbert, 2024a). QKD leverages quantum communication networks to generate cryptographic keys, providing an additional layer of security to blockchain communications (Gilbert & Gilbert, 2024i). However, implementing QKD comes with practical challenges, including limited range, key distribution issues, errors, and high costs associated with deployment (Gilbert & Gilbert, 2024i; Dwivedi et al., 2024).

Popular public-key cryptography algorithms such as RSA and Elliptic Curve Cryptography (ECC) may be susceptible to quantum computing attacks, prompting ongoing research into post-quantum cryptography to develop quantum-resistant algorithms (Acar et al., 2018). Unlike classical hardware, quantum computers use principles of superposition and entanglement, giving them the computational power to potentially break current cryptographic systems. This raises important questions about how widely-used cryptographic algorithms will need to evolve in order to withstand quantum attacks.

8. Future Directions in Cryptographic Algorithms

Revisiting the assumption of static encryption naturally leads to the concept of secure protocols that evolve during an ongoing communication session (Mavroeidis et al., 2018). Instead of relying on a single, static cryptographic protocol for a given public key and message, adaptive public-key encryption (APE) can be employed. In APE, publicly available information, aside from the plaintext, is adjusted based on previous queries. Historically, the distinction between chosen ciphertext attack (CCA) and chosen plaintext attack (CPA) security was viewed as a theoretical constraint. This constraint suggested that public-key encryption, even if sufficiently secure, couldn't convert a CPA attack into a CCA attack (Gilbert & Gilbert, 2024b).

The design possibilities for cryptographic algorithms have been somewhat restricted by the requirement that the algorithms themselves be publicly available (Baseri, Hafid & Makrakis, 2024). This challenge has inspired the idea of using a smaller set of cryptographic protocols while allowing the key generation and updating mechanisms to be adaptive (Andronikos & Sirokofskich, 2023; Gilbert, Auodo & Gilbert, 2024). One advantage of using a fixed set of cryptographic protocols is that machine learning algorithms can be applied to generate new, secure protocols. Another approach involves adapting the cryptographic framework based on the communication channel properties, with quantum key distribution (QKD) being a widely studied example.

8.1. Quantum Cryptography

This section begins by reviewing the development and evolution of cryptographic algorithms in response to growing cyber threats, including their application in digital currencies. It further emphasizes that post-quantum cryptography will be a critical technology in the future, presenting significant challenges for the cryptographic community. The chapter discusses several public key proposals and highlights improvements in security for email communication (Gilbert & Gilbert, 2024c). However, it also notes that issues related to standards, certification, and economic feasibility must be addressed. Germany's federal cybersecurity agency, BSI, has made several recommendations, including a goal to finalize a list of "safe" cryptographic applications by 2025.

Quantum computers are anticipated to vastly outperform classical computers in terms of computational speed and efficiency (Baseri, Hafid & Makrakis, 2024). This computational advantage has wide-ranging implications for fields such as material science, drug discovery, and optimization. More importantly, quantum computers pose a significant threat to traditional cryptographic methods (Gilbert & Gilbert, 2024m). For instance, if quantum computers can efficiently factor large integers or compute discrete logarithms, widely used cryptographic algorithms like RSA and ECC will be rendered ineffective. This potential scenario makes the development of post-quantum cryptography urgent. Post-quantum cryptography aims to complement traditional encryption techniques, ensuring secure communication systems remain robust against quantum-enabled adversaries (Chen et al., 2022).

8.2. Biometric Cryptography

Biometric systems use unique physical and behavioral traits, such as facial features, fingerprints, and voice recognition, to authenticate or identify individuals (Zhang et al., 2018). Biometric cryptosystems, on the other hand, establish a link between biometric data and cryptographic keys, which can then be employed for encryption or decryption. For effective key management in cryptographic systems, it is essential that biometric features are consistently used within acceptable error limits throughout the system's lifecycle, even after events such as noise interference or damage to the measurements (Zhang et al., 2018). Electroencephalography (EEG) has emerged as a flexible and secure alternative to traditional biometrics for authentication and recognition, offering enhanced security in modern access control systems (Gilbert & Gilbert, 2024d). However, EEG signals may vary across different points on an individual's head, potentially allowing an attacker to launch a replay attack by deceiving the detection system with different signals. Despite this, the physiological uniqueness of EEG signals ensures individual differences, making it possible to resolve this issue by using a personalized identity key. This secure sketch of the EEG signal enhances the security of EEG-based biometrics through human tolerance.

Traditional encryption schemes (ECs) typically require manual operations to generate cryptographic keys, which can limit their usability, especially when users themselves cannot retrieve the corresponding key when needed. To enable revocable biometrics, it is crucial to consider key systems that users can easily change while maintaining the probabilistic verification of biometric information. In this context, combining secret data with normal data to generate a key ensures that encrypted biometric cryptosystems (EBCs) can achieve revocable authentication. For reliable verification, keys generated in various ways should be integrated to support both biometric and cryptographic requirements ((Omotosho et al.,2018; Gilbert & Gilbert, 2024e).

8.3. AI and Machine Learning in Cryptography

Machine Learning (ML) and Artificial Intelligence (AI) have yet to become widespread components of mainstream cybersecurity solutions. However, AI's potential in cybersecurity is vast, offering benefits such as continuous risk assessment, real-time tool design and modification based on network topologies and protocols, and cryptography vulnerability mapping (McDaniel & Koushanfar, 2023). Additionally, AI-based solutions can address modern cybersecurity challenges like Public Key Infrastructure (PKI) rethinking, the threat posed by quantum computing, and managing network elements such as Software Defined Networks (SDN) and Network Function Virtualization (NFV) systems. AI systems are valuable in assessing, classifying, and defending networks by understanding their real-time behaviors and operations. As a result, embedding AI algorithms directly into hardware systems, such as Systems on Chips (SoCs), is increasingly seen as a necessary step for enhancing network security (Gilbert & Gilbert, 2024c; Nasser & Nassar, 2023).

Machine Learning and AI are already applied in high-tech solutions across various fields, including biological process analysis through machine learning and statistical assessment models (SAMs)(Nasser & Nassar, 2023). These technologies are anticipated to drive advancements leading to technological singularity, a point where AI systems may create challenges beyond human capability to solve. In the realm of cybersecurity, the abilities of defenders (armed with AI tools) are often asymmetrical compared to those of attackers, who manage to exploit just a few refined tools. It is suggested that technologies such as AI, edge systems, 5G standalone networks, robotics, biotechnological factors, deep space technologies, nuclear matters, and unmanned aircraft systems (UAS) will shape the future of technology-driven policies (Radanliev et al., 2022).

9. Conclusion and Implications for Cybersecurity

In the current market landscape, both companies and governments are becoming increasingly aware of the approaching reality of quantum computing. The Stone–Weierstrass theorem in quantum-secure encryption suggests that there may soon be a need to transition from traditional cryptosystems to quantum-resistant ones, either through gradual evolution or an abrupt overhaul. The former could resemble the shift from symmetric to asymmetric keys, with systems adapting accordingly. However, the latter may necessitate a complete redevelopment of cryptographic layers, impacting devices, networks, and web platforms. This shift has already prompted market demands for migrating RSA to quantum-resistant algorithms and implementing hybrid encryption systems (Radanliev et al., 2022).

Cryptosystems are essential in defending against adversarial activities, such as exploiting vulnerabilities, stealing data, and disrupting network operations. Public key cryptosystems, in particular, are critical in various applications, including secure email, SSL communications, anonymity networks, and digital signatures. Ensuring the security of communication infrastructures requires addressing potential vulnerabilities and implementing proposed solutions (Radanliev et al., 2022). Over the past four decades, the widespread adoption of public key cryptography has revealed numerous threats, prompting the development of effective countermeasures. However, cryptosystems must continue to evolve to meet emerging cyber threats. This chapter highlights some of the challenges arising from Shor's quantum algorithm and emphasizes the need to strengthen elliptic-curve cryptosystems like ECIES. Moreover, it discusses the importance of hybrid encryption methods in safeguarding governments and businesses from ransomware attacks that utilize elliptic-curve cryptography and RSA (Radanliev et al., 2022).

References

1. Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security*, 16(1), 11.
2. Abilimi, C. A., & Adu-Manu, K. S. (2013). *Examining the impact of Information and Communication Technology capacity building in High School education in Ghana.* International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 2 Issue 9, September – 2013.
3. Abilimi, C. A. & Yeboah, T. (2013). Assessing the challenges of Information and Communication Technology in educational development in High Schools in Ghana. International Journal of Engineering Research & Technology (IJERT).ISSN: 2278-0181, Vol. 2 Issue 11, November – 2013.
4. Abilimi,C.A, Asante,M, Opoku-Mensah, E & Boateng, F.O. (2015). Testing for Randomness in Pseudo Random Number Generators Algorithms in a Cryptographic Application.Computer Engineering and Intelligent Systems, www.iiste.org, ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.9, 2015.
5. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific and Research Publications*, 8(7), 495–516.
6. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR)*, 51(4), 1–35.
7. Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. *Cluster Computing*, 1–16.
8. Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods.
9. Albrecht, M., & Ducas, L. (2021). Lattice attacks on NTRU and LWE: A history of refinements. *Cryptology ePrint Archive*.
10. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, 12(2), 256–272.
11. Algazy, K., Sakan, K., Khompysh, A., & Dyusenbayev, D. (2024). Development of a New Post-Quantum Digital Signature Algorithm: Syrga-1. *Computers*, 13(1), 26.
12. Alhaj, A. A., Alrabea, A., & Jawabreh, O. (2024). Efficient and secure data transmission: Cryptography techniques using ECC. *Indonesian Journal of Electrical Engineering and Computer Science*, 36(1), 486–492.
13. Alquwayzani, A. A., & Albuali, A. A. (2024). A Systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT.
14. Al-Shabi, M. A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, 9(3), 576–589.
15. Anwar, M. N. B., Hasan, M., Hasan, M. M., Loren, J. Z., & Hossain, S. T. (2019). Comparative study of cryptography algorithms and its applications. *International Journal of Computer Networks and Communications Security*, 7(5), 96–103.
16. Andronikos, T., & Sirokofskich, A. (2023). An entanglement-based protocol for simultaneous reciprocal information exchange between 2 players. *Electronics*, 12(11), 2506.
17. Arun, A., Bonneau, J., & Clark, J. (2022, December). Short-lived zero-knowledge proofs and signatures. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 487–516). Springer Nature Switzerland.
18. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
19. Aumasson, J. P. (2024). *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, Inc.

20. Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. *Security and Communication Networks*, 2020, 8863345.

21. Babu, P. R., Kumar, S. A., Reddy, A. G., & Das, A. K. (2024). Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges. *Computer Science Review*, 54, 100676.

22. Banerjee, K., & Saha, S. (2024). Blockchain signatures to ensure information integrity and non-repudiation in the digital era: A comprehensive study. *International Journal of Computing and Digital Systems*, 16(1), 1–12.

23. Bansod, S., & Ragha, L. (2022). Challenges in making blockchain privacy compliant for the digital world: Some measures. *Sādhanā*, 47(3), 168.

24. Baseri, Y., Hafid, A. S., & Makrakis, D. (2024a). Privacy-Enhanced Adaptive Authentication: User Profiling with Privacy Guarantees. *arXiv preprint arXiv:2410.20555*.

25. Baseri, Y., Chouhan, V., & Hafid, A. (2024b). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security*, 103883.

26. Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., & Daniel, S. J. (2022). Post quantum cryptography: Techniques, challenges, standardization, and directions for future research. *arXiv preprint arXiv:2202.02826*.

27. Belhadjoudja, M. C. (2021). Chaos synchronization using nonlinear observers with applications to cryptography. *arXiv preprint arXiv:2108.02577*.

28. Bhowmik, A., & Menon, U. (2021). An adaptive cryptosystem on a finite field. *PeerJ Computer Science*, 7, e637.

29. Chen, F., Wang, J., Li, J., Xu, Y., Zhang, C., & Xiang, T. (2022). TrustBuilder: A non-repudiation scheme for IoT cloud applications. *Computers & Security*, 115, 102664.

30. Ciulei, A. T., Crețu, M. C., & Simion, E. (2022). Preparation for post-quantum era: A survey about blockchain schemes from a post-quantum perspective. *Cryptology ePrint Archive*.

31. Danquah, P., & Kwabena-Adade, H. (2020). Public key infrastructure: An enhanced validation framework. *Journal of Information Security*, 11(4), 241–260.

32. Das, P., Hesse, J., & Lehmann, A. (2022). DPaSE: Distributed password-authenticated symmetric-key encryption, or how to get many keys from one password. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (pp. 682–696).

33. De Leon, N. P., Itoh, K. M., Kim, D., Mehta, K. K., Northup, T. E., Paik, H., ... & Steuerman, D. W. (2021). Materials challenges and opportunities for quantum computing hardware. *Science*, 372(6539), eabb2823.

34. Dwivedi, Y. K., Pandey, N., Currie, W., & Micu, A. (2024). Leveraging ChatGPT and other generative artificial intelligence (AI)-based applications in the hospitality and tourism industry: Practices, challenges and research agenda. *International Journal of Contemporary Hospitality Management*, 36(1), 1–12.

35. El-Dalahmeh, A., El-Dalahmeh, M., Razzaque, M. A., & Li, J. (2024). Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. *Security and Privacy*, e446.

36. Frank, E. (2024). *Cryptographic Algorithms in Secure Text Steganography* (No. 13259). EasyChair.

37. Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. *IEEE Access*, 8, 152351–152366.

38. Gilbert, C.(2012). The Quest of Father and Son: Illuminating Character Identity, Motivation, and Conflict in Cormac McCarthy's *The Road.* English Journal, Volume 102, Issue Characters and Character, p. 40 - 47. https://doi.org/10.58680/ej201220821.

39. Gilbert, C. (2018). Creating Educational Destruction: A Critical Exploration of Central Neoliberal Concepts and Their Transformative Effects on Public Education. *The Educational Forum*, *83*(1), 60–74. https://doi.org/10.1080/00131725.2018.1505017.

40. Gilbert, C. & Gilbert, M.A.(2024a).Unraveling Blockchain Technology: A Comprehensive Conceptual Review. International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and ISSN Approved), ISSN:2349-5162, Vol.11, Issue 9, page no. ppa575-a584, September-2024, Available at : http://www.jetir.org/papers/JETIR2409066.pdf

41. Gilbert, C. & Gilbert, M.A.(2024b).Strategic Framework for Human-Centric AI Governance: Navigating Ethical, Educational, and Societal Challenges. International Journal of Latest Technology in Engineering Management & Applied Science, 13(8), 132-141. https://doi.org/10.51583/IJLTEMAS.2024.130816

42. Gilbert, C. & Gilbert, M.A.(2024c).The Impact of AI on Cybersecurity Defense Mechanisms: Future Trends and Challenges.Global Scientific Journals.ISSN 2320-9186,12(9),427-441.

https://www.globalscientificjournal.com/researchpaper/The_Impact_of_AI_on_Cybersecurity_Defense_Mechanisms_Future_Trends_and_Challenges_.pdf.

43. Gilbert, C. & Gilbert, M.A. (2024d). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, *3*(9), 9-9.

44. Gilbert, C. & Gilbert, M.A.(2024e).Transforming Blockchain: Innovative Consensus Algorithms for Improved Scalability and Security. International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.11, Issue 10, page no.b299-b313, October-2024, Available :http://www.jetir.org/papers/JETIR2410134.pdf

45. Gilbert, C. & Gilbert, M.A. (2024f). Future Privacy Challenges: Predicting the Agenda of Webmasters Regarding Cookie Management and Its Implications for User Privacy. International Journal of Advanced Engineering Research and Science, ISSN (Online): 2455-9024, Volume 9, Issue 4, pp. 95-106.

46. Gilbert, C., & Gilbert, M. A. (2024g). Navigating the Dual Nature of Deepfakes: Ethical, Legal, and Technological Perspectives on Generative Artificial Intelligence (AI) Technology. *International Journal of Scientific Research and Modern Technology*, *3*(10). https://doi.org/10.38124/ijsrmt.v3i10.54

47. Gilbert, C., & Gilbert, M. A. (2024h).Revolutionizing Computer Science Education: Integrating Blockchain for Enhanced Learning and Future Readiness. International Journal of Latest Technology in Engineering, Management & Applied Science, ISSN 2278-2540, Volume 13, Issue 9, pp.161-173.

48. Gilbert, C. & Gilbert, M.A. (2024i). Unlocking Privacy in Blockchain: Exploring Zero-Knowledge Proofs and Secure Multi-Party Computation Techniques. Global Scientific Journal (ISSN 2320-9186) 12 (10), 1368-1392.

49. Gilbert, C. & Gilbert, M.A. (2024j).The Role of Artificial Intelligence (AI) in Combatting Deepfakes and Digital Misinformation. International Research Journal of Advanced Engineering and Science (ISSN: 2455-9024), Volume 9, Issue 4, pp. 170-181.

50. Gilbert, C. & Gilbert, M.A.(2024k). AI-Driven Threat Detection in the Internet of Things (IoT), Exploring Opportunities and Vulnerabilities. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 219-236.

51. Gilbert, C., & Gilbert, M. A. (2024l). The security implications of artificial intelligence (AI)-powered autonomous weapons: Policy recommendations for international regulation. *International Research Journal of Advanced Engineering and Science*, *9*(4), 205–219.

52. Gilbert, C., & Gilbert, M. A. (2024m). The role of quantum cryptography in enhancing cybersecurity. *International Journal of Research Publication and Reviews*, *5*(11), 889–907. https://www.ijrpr.com

53. Gilbert, C., & Gilbert, M. A. (2024n). Bridging the gap: Evaluating Liberia's cybercrime legislation against international standards. *International Journal of Research and Innovation in Applied Science (IJRIAS)*, *9*(10), 131–137. https://doi.org/10.51584/IJRIAS.2024.910013

54. Gilbert, C., & Gilbert, M. A. (2024o). The Effectiveness of Homomorphic Encryption in Protecting Data Privacy. *International Journal of Research Publication and Reviews*, *5*(11), 3235-3256. https://www.ijrpr.com.

55. Gilbert, C., & Gilbert, M. A. (2024p).CRYPTOGRAPHIC FOUNDATIONS AND CYBERSECURITY IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY.*Global Scientific Journals,*ISSN 2320-9186,12(11),464-487. https://www.globalscientificjournal.com

56. Gilbert, C., & Gilbert, M. A. (2024q). Advancing privacy standards through education: The role of academic initiatives in enhancing privacy within Cardano's blockchain ecosystem. *International Research Journal of Advanced Engineering and Science, 9*(4), 238–251.

57. Gilbert, C., & Gilbert, M. A. (2024r). Leveraging artificial intelligence (AI) by a strategic defense against deepfakes and digital misinformation. *International Journal of Scientific Research and Modern Technology, 3*(11). https://doi.org/10.38124/ijsrmt.v3i11.76

58. Gilbert, C., & Gilbert, M. A. (2024s). Evaluation of the efficiency of advanced number generators in cryptographic systems using a comparative approach. *International Journal of Scientific Research and Modern Technology, 3*(11). https://doi.org/10.38124/ijsrmt.v3i11.77

59. Gilbert, C., & Gilbert, M. A. (2024t). Cybersecurity risk management frameworks for critical infrastructure protection. *International Journal of Research Publication and Reviews, 5*(12), 507–533. https://www.ijrpr.com/

60. Gilbert, M.A., Oluwatosin, S. A., & Gilbert, C.(2024). An investigation into the types of role-based relationships that exist between lecturers and students in universities across southwestern nigeria: a sociocultural and institutional analysis. Global Scientific Journal, ISSN 2320-9186, Volume 12, Issue 10, pp. 263-280.

61. Gilbert, M.A., Auodo, A. & Gilbert, C.(2024). Analyzing Occupational Stress in Academic Personnel through the Framework of Maslow's Hierarchy of Needs. International Journal of Research Publication and Reviews, Vol 5, no 11, pp 620-630.

62. Gill, S. S., Wu, H., Patros, P., Ottaviani, C., Arora, P., Pujol, V. C., ... & Buyya, R. (2024). Modern computing: Vision and challenges. *Telematics and Informatics Reports*, 100116.

63. Gour, A., Malhi, S. S., Singh, G., & Kaur, G. (2024). Hybrid cryptographic approach: For secure data communication using block cipher techniques. In *E3S Web of Conferences* (Vol. 556, p. 01048). EDP Sciences.

64. Hagras, E. A., Aldosary, S., Khaled, H., & Hassan, T. M. (2023). Authenticated public key elliptic curve based on deep convolutional neural network for cybersecurity image encryption application. *Sensors*, 23(14), 6589.

65. Halak, B., Yilmaz, Y., & Shiu, D. (2022). Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. *IEEE Access*, 10, 76707–76719.

66. Hasan, F., Simpson, L., Rezazadeh Baee, M. A., Islam, C., Ziaur, R., Armstrong, W., ... & McKague, M. (2023). Migrating to post-quantum cryptography: A framework using security dependency analysis.

67. Henson, M., & Taylor, S. (2014). Memory encryption: A survey of existing techniques. *ACM Computing Surveys (CSUR)*, 46(4), 1–26.

68. Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021). Systematic and critical review of RSA-based public key cryptographic schemes: Past and present status. *IEEE Access*, 9, 155949–155976.

69. Irviani, R., & Muslihudin, M. (2018). Nur algorithm on data encryption and decryption. *International Journal of Engineering & Technology*, 7(2.26), 109–118.

70. Jiang, L., Cao, Y., Yuan, C., Sun, X., & Zhu, X. (2019). An effective comparison protocol over encrypted data in cloud computing. *Journal of Information Security and Applications*, 48, 102367.

71. Khan, N. S., & Chishti, M. A. (2020). Security challenges in fog and IoT, blockchain technology and cell tree solutions: A review. *Scalable Computing: Practice and Experience*, 21(3), 515–542.

72. Khaleel, Y. L., Habeeb, M. A., Albahri, A. S., Al-Quraishi, T., Albahri, O. S., & Alamoodi, A. H. (2024). Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. *Journal of Intelligent Systems*, 33(1), 20240153.

73. Koutsos, V., Papadopoulos, D., Chatzopoulos, D., Tarkoma, S., & Hui, P. (2021). Agora: A privacy-aware data marketplace. *IEEE Transactions on Dependable and Secure Computing*, 19(6), 3728–3740.

74. Kumar, A., Bhatia, S., Kaushik, K., Gandhi, S. M., Devi, S. G., Diego, A. D. J., & Mashat, A. (2021). Survey of promising technologies for quantum drones and networks. *IEEE Access*, 9, 125868–125911.

75. Kwame, A. E., Martey, E. M., & Chris, A. G. (2017). Qualitative assessment of compiled, interpreted and hybrid programming languages. *Communications on Applied Electronics*, *7*(7), 8-13.

76. Lavanya, K. (2018). CLOAK: A flow-based encryption protocol for mobile cloud computing. *IJRAR-International Journal of Research and Analytical Reviews*, 5(4), 499–506.

77. Lozi, R. (2023). Survey of recent applications of the chaotic Lozi map. *Algorithms*, 16(10), 491.

78. Mahto, D., & Yadav, D. K. (2017). RSA and ECC: A comparative analysis. *International Journal of Applied Engineering Research*, 12(19), 9053–9061.

79. Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, 190(1), 1–69.

80. Mago, N. (2016). PMAC: A fully parallelizable MAC algorithm.

81. Marks, P. (2024). Review of *Behind the Enigma* by John Ferris.

82. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

83. McDaniel, P., & Koushanfar, F. (2023). Secure and trustworthy computing 2.0 vision statement. *arXiv preprint arXiv:2308.00623*.

84. Mohamed, K. S., & Mohamed, K. S. (2020). Cryptography concepts: Confidentiality. In *New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA* (pp. 13–39).

85. Mohit, Kaur, S., & Singh, M. (2024). Design and implementation of blockchain-based supply chain framework with improved traceability, privacy, and ownership. *Cluster Computing*, 27(3), 2345–2363.

86. Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: A survey. *Wireless Networks*, 27(2), 1515–1555.

87. Müller, J., Brinkmann, M., Poddebniak, D., Böck, H., Schinzel, S., Somorovsky, J., & Schwenk, J. (2019). "Johnny, you are fired!"—Spoofing OpenPGP and S/MIME signatures in emails. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 1011–1028).

88. Nasser, Y., & Nassar, M. (2023). Toward hardware-assisted malware detection utilizing explainable machine learning: A survey. *IEEE Access*, 11, 131273–131288.

89. Omotosho, A., Emuoyibofarhe, J., Ayegba, P., & Meinel, C. (2018). E-prescription in Nigeria: A survey. *Journal of Global Pharma Technology*.

90. Opoku-Mensah, E., Abilimi, C. A., & Boateng, F. O. (2013). Comparative analysis of efficiency of fibonacci random number generator algorithm and gaussian Random Number Generator Algorithm in a cryptographic system. *Comput. Eng. Intell. Syst*, *4*, 50-57.

91. Opoku-Mensah, E., Abilimi, A. C., & Amoako, L. (2013). The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service. *International Journal on Computer Science and Engineering (IJCSE)*, 760-769.

92. Park, J. Y., Moon, Y. H., Lee, W., Kim, S. H., & Sakurai, K. (2021). A survey of polynomial multiplication with RSA-ECC coprocessors and implementations of NIST PQC Round3 KEM algorithms in Exynos2100. *IEEE Access*, 10, 2546–2563.

93. Patel, D., Patel, B., Vasa, J., & Patel, M. (2023, April). A comparison of the key size and security level of the ECC and RSA algorithms with a focus on cloud/fog computing. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 43–53). Springer Nature Singapore.

94. Peechara, R. R., & Sucharita, V. (2021). A chaos theory inspired, asynchronous two-way encryption mechanism for cloud computing. *PeerJ Computer Science*, 7, e628.

95. Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., & Santos, O. (2022). Digital twins: Artificial intelligence and the IoT cyber-physical systems in Industry 4.0. *International Journal of Intelligent Robotics and Applications*, 6(1), 171–185.

96. Radanliev, P., & De Roure, D. (2023). New and emerging forms of data and technologies: Literature and bibliometric review. *Multimedia Tools and Applications*, 82(2), 2887–2911.

97. Raeisi-Varzaneh, M., Dakkak, O., Alaidaros, H., & Avci, İ. (2024). Internet of things: Security, issues, threats, and assessment of different cryptographic technologies. *Journal of Communications*, 19(2).

98. Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. *Ad Hoc Networks*, 146, 103159.

99. SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2024). A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos, Solitons & Fractals*, 178, 114361.

100. Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers in Physics*, 12, 1456491.

101. Santoso, B., & Oohama, Y. (2019). Information theoretic security for Shannon cipher system under side-channel attacks. *Entropy*, 21(5), 469.

102. Sarkar, A., Ganguly, S., Sarkar, P. S., & Chatterjee, S. R. (2024). PUF-based authentication system with resilience against multi-faceted attacks for blockchain-based IoT networks. In *2024 IEEE 3rd World Conference on Applied Intelligence and Computing (AIC)* (pp. 1279–1284). IEEE.

103. Sarkar, A., Chatterjee, S. R., & Chakraborty, M. (2021). Role of cryptography in network security. In *The "Essence" of Network Security: An End-to-End Panorama* (pp. 103–143).

104. Sayakkara, A., Le-Khac, N. A., & Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, 29, 43–54.

105. Shabbir, A., Shabbir, M., Rizwan, M., & Ahmad, F. (2019). Ensuring the confidentiality of nuclear information at cloud using modular encryption standard. *Security and Communication Networks*, 2019, 2509898.

106. Shah, M. S. M., Leau, Y. B., Anbar, M., & Bin-Salem, A. A. (2023). Security and integrity attacks in named data networking: A survey. *IEEE Access*, 11, 7984–8004.

107. Sharma, S., Meyer, R. T., & Asher, Z. D. (2024). AEPF: Attention-enabled point fusion for 3D object detection. *Sensors*, 24(17), 5841.

108. Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. *Transactions on Emerging Telecommunications Technologies*, 35(1), e4884.

109. Singh, P., Choudhary, N., Samnotra, B., Bhel, S., Sharma, S., Kour, H., ... & Kumar, S. (2024). Understanding RSA algorithm in cryptography.

110. Suhail, S., Hussain, R., Khan, A., & Hong, C. S. (2020). On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. *IEEE Internet of Things Journal*, 8(1), 1–17.

111. Talukder, M. A., Hasan, K. F., Islam, M. M., Uddin, M. A., Akhter, A., Yousuf, M. A., ... & Moni, M. A. (2023). A dependable hybrid machine learning model for network intrusion detection. *Journal of Information Security and Applications*, 72, 103405.

112. Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, 22, 100759.

113. Tolba, Z. (2024). Cryptanalysis and improvement of multimodal data encryption by machine-learning-based system. *arXiv preprint arXiv:2402.15779*.

114. Tom, J. J., Anebo, N. P., Onyekwelu, B. A., Wilfred, A., & Eyo, R. E. (2023). Quantum computers and algorithms: A threat to classical cryptographic systems. *International Journal of Engineering and Advanced Technology*, 12(5), 25–38.

115. Tsipenyuk, G. Y. (2018). *Evaluation of Decentralized Email Architecture and Social Network Analysis Based on Email Attachment Sharing* (No. UCAM-CL-TR-918). University of Cambridge, Computer Laboratory.

116. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic curve cryptography: Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, 47, 100530.

117. Umay, A. (2024). AI in academic research. In *Impact of Artificial Intelligence on Society* (p. 81).

118. Van de Graaf, J., & Lenstra, A. K. (2024). Delphi: Sharing assessments of cryptographic assumptions. *Cryptology ePrint Archive*.

119. WARSONO, W. (2016). *Analysis of Commissive Utterances in The Imitation Game Movie* (Doctoral dissertation, Sekolah Tinggi Bahasa Asing JIA).

120. Wille, R., Berent, L., Forster, T., Kunasaikaran, J., Mato, K., Peham, T., ... & Burgholzer, L. (2024). The MQT handbook: A summary of design automation tools and software for quantum computing. *arXiv preprint arXiv:2405.17543*.

121. Wollinger, T., Guajardo, J., & Paar, C. (2004). Security on FPGAs: State-of-the-art implementations and attacks. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3), 534–574.

122. Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A review of the present cryptographic arsenal to deal with post-quantum threats. *Procedia Computer Science*, 215, 834–845.

123. Yeboah, T., Opoku-Mensah, E., & Abilimi, C.A.(2013a). A Proposed Multiple Scan Biometric-Based Registration System for Ghana Electoral Commission. *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, *2*(7).

124. Yeboah, D. T., Odabi, I., & Abilimi Odabi, M. C. A. A. (2016). *Utilizing divisible load scheduling theorem in round robin algorithm for load balancing in cloud environment*.

125. Yeboah, T., Opoku-Mensah, E., & Abilimi, C. A. (2013b).Automatic Biometric Student Attendance System: A Case Study Christian Service University College. *Journal of Engineering Computers & Applied Sciences*, 2(6), 117-121.

126. Yeboah T. & Abilimi C.A. (2013).*Using Adobe Captivate to creative Adaptive Learning Environment to address individual learning styles: A Case study Christian Service University*, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,www.ijert.org, “2(11).

127. Zeadally, S., Das, A. K., & Sklavos, N. (2021). Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*, 14, 100075.

128. Zhang, Q., Jia, S., Chang, B., & Chen, B. (2018). Ensuring data confidentiality via plausibly deniable encryption and secure deletion—A survey. *Cybersecurity*, 1, 1–20.

129. Zunaidi, M. R., Sayakkara, A., & Scanlon, M. (2024). Revealing IoT cryptographic settings through electromagnetic side-channel analysis. *Electronics*, 13(8), 1579.