ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

Constructing a CPA-Secure: Pseudo-Random Permutations and Block Ciphers, Modes of Operation, Security Against Chosen-Ciphertext Attacks (CCA)

Idowu Mayowa Opakunle[1]; Ojoawo Akinwale Olusola[2]; Oladeji Oluwakayode Paul[3]; Alabi Adewale Abayomi[4]

[1]Computer Science Lead City University, Ibadan
[2] Computer Science Dept, Adeseun Ogundoyin Polytechnic, Eruwa, Nigeria
[3]Great Cities Education Academy, Edo
[4]Computer Engineering Adeseun Ogundoyin Polytechinc Eruwa. Nigeria

Publication Date: 2026/08/01

Abstract: This paper examines symmetric-key encryption as a layered security construction, tracing how cryptographic guarantees propagate from primitive to protocol. The study is conducted as a structured literature review of foundational and recent (2021–2025) cryptographic research on block cipher modes of operation and their resistance to chosen-plaintext and chosen-ciphertext attacks. At the foundation lies the block cipher, modeled as a pseudorandom permutation (PRP) whose security rests on cryptanalytic conjecture rather than provable hardness. Building on this, modes of operation including ECB, CBC, CFB, OFB, and CTR combine block-cipher calls to encrypt arbitrary-length messages, with security formally reduced to the underlying PRP assumption under indistinguishability against chosen-plaintext attack (IND-CPA). The review finds that while CPA security is necessary, it is insufficient for real-world deployment, since adversaries in network settings routinely gain oracle-like access to decryption; this is evidenced by recurring vulnerabilities such as padding-oracle attacks and related exploits against CBC-mode TLS. It further finds that the stronger requirement of indistinguishability under chosen-ciphertext attack (IND-CCA) is achieved through authenticated constructions such as Encrypt-then-MAC and, increasingly in current practice, integrated Authenticated Encryption with Associated Data (AEAD) schemes such as AES-GCM. The paper concludes that authenticated encryption should be the default standard in protocol design, closing the theoretical–practical gap that has historically enabled real-world cryptographic exploits.

Keywords: *Symmetric-Key Cryptography; Pseudorandom Permutation (PRP); Modes of Operation; Chosen-Plaintext Attack (CPA); Chosen-Ciphertext Attack (CCA); Authenticated Encryption (AEAD); Padding-Oracle Attack*

How to Cite: Idowu Mayowa Opakunle; Ojoawo Akinwale Olusola; Oladeji Oluwakayode Paul; Alabi Adewale Abayomi (2026) Constructing a CPA-Secure: Pseudo-Random Permutations and Block Ciphers, Modes of Operation, Security Against Chosen-Ciphertext Attacks (CCA). *International Journal of Innovative Science and Research Technology*, 11(7), 2368-2376. https://doi.org/10.38124/ijisrt/26jul1487

I. INTRODUCTION

The rapid advancement of digital technologies has significantly increased the demand for secure communication systems capable of protecting sensitive information against unauthorized access. Applications such as electronic banking, cloud computing, Internet of Things (IoT), healthcare information systems, and secure messaging services rely extensively on symmetric-key cryptography because of its computational efficiency and ability to encrypt large volumes of data with minimal processing overhead (Mouha, 2021; National Institute of Standards and Technology [NIST], 2023).

Among symmetric encryption algorithms, the Advanced Encryption Standard (AES) remains the globally accepted standard for protecting confidential information. Since its standardization, AES has undergone extensive cryptanalytic evaluation, and recent reviews by NIST reaffirm that no practical attacks capable of compromising the full AES algorithm have been identified, making it the preferred block cipher for government, commercial, and industrial applications (NIST, 2023).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

However, a block cipher alone cannot securely encrypt messages of arbitrary length. Practical encryption requires combining the underlying block cipher with an appropriate mode of operation, such as Cipher Block Chaining (CBC), Counter (CTR), Cipher Feedback (CFB), Output Feedback (OFB), or Galois/Counter Mode (GCM). The security achieved by these modes depends not only on the strength of the underlying block cipher but also on their correct implementation, proper initialization vector (IV) generation, nonce management, and authentication mechanisms (Mouha & Dworkin, 2024).

Although many traditional block cipher modes satisfy the security notion of indistinguishability under chosen-plaintext attacks (IND-CPA), modern communication systems increasingly operate in hostile environments where attackers can intercept, modify, replay, or inject ciphertexts into communication channels. Under these conditions, confidentiality alone is insufficient because active adversaries may exploit weaknesses in protocol implementation through padding-oracle attacks, nonce misuse, timing attacks, or ciphertext manipulation. Consequently, modern cryptographic protocols increasingly adopt authenticated encryption schemes that provide resistance against chosen-ciphertext attacks (IND-CCA) while simultaneously ensuring confidentiality, integrity, and authenticity (Kampanakis et al., 2024).

In practical terms, this layered chain of guarantees is what protects something as ordinary as the padlock icon shown during online banking or online shopping. When a browser displays that padlock, it signals that the Transport Layer Security (TLS) protocol is using exactly this progression a block cipher trusted to behave as a pseudorandom permutation, combined into a CPA-secure mode of operation, and wrapped in an authenticated encryption scheme resistant to chosen-ciphertext attacks to keep transaction data both unreadable and untamperable while it travels across the network.

➢ *Statement of the Problem*

Despite continuous improvements in symmetric-key cryptography, many deployed communication systems remain vulnerable because encryption modes that provide confidentiality under chosen-plaintext attacks do not necessarily guarantee protection against active adversaries. Numerous real-world attacks have demonstrated that improper implementation of block cipher modes or the absence of message authentication can expose encrypted systems to ciphertext manipulation and information leakage. Consequently, misunderstanding the distinction between CPA-secure and CCA-secure encryption continues to contribute to weaknesses in protocol design and secure system implementation.

➢ *Research Gap*

Existing literature has extensively examined block ciphers, pseudorandom permutations, block cipher modes of operation, and authenticated encryption as independent research topics. Recent reviews have focused on evaluating AES security, lightweight cryptography, authenticated encryption schemes, or implementation challenges individually (Mouha, 2021; Kaur et al., 2023). However, relatively few studies provide a comprehensive review explaining how cryptographic security evolves from pseudorandom permutations through CPA-secure block cipher modes to CCA-secure authenticated encryption within a single conceptual framework.

This study addresses this gap by presenting an integrated review of the theoretical foundations, security properties, and practical implications of modern symmetric-key encryption, demonstrating how these concepts collectively contribute to secure communication systems.

➢ *Aim of the Study*

The aim of this study is to examine how modern symmetric-key encryption achieves secure communication by progressing from pseudorandom permutations and block ciphers through CPA-secure modes of operation to CCA-secure authenticated encryption schemes.

➢ *Objectives of the Study*

The specific objectives are to:

- Examine the role of pseudorandom permutations in the construction of secure block ciphers;
- Analyze the security properties of major block cipher modes of operation under chosen-plaintext attacks;
- Investigate the limitations of CPA-secure encryption and the security requirements of chosen-ciphertext attack resistance;
- Evaluate authenticated encryption techniques used to achieve confidentiality, integrity, and authentication in modern cryptographic protocols.

➢ *Significance of the Study*

This study contributes to the understanding of modern symmetric encryption by presenting a comprehensive review that links theoretical cryptographic foundations with practical protocol security. The findings will benefit researchers, students, software developers, cybersecurity professionals, and system designers by clarifying the relationship between block ciphers, modes of operation, CPA security, CCA security, and authenticated encryption.

II. RELATED WORKS

➢ *Recent Advances in Block Ciphers and Modes of Operation*

Symmetric-key cryptography remains the dominant approach for protecting digital information because of its computational efficiency and suitability for high-speed communication systems. Recent reviews by the National Institute of Standards and Technology (NIST) reaffirm that the Advanced Encryption Standard (AES) continues to provide strong security for government and commercial applications, while emphasizing that the practical security of encrypted systems depends not only on the underlying block cipher but also on the correct selection and implementation of block cipher modes of operation (Mouha & Dworkin, 2024). NIST further recommends continuous evaluation of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

standardized modes to address emerging implementation challenges and evolving security requirements.

Modern communication systems increasingly employ modes such as CBC, CTR, GCM, and XTS to provide confidentiality across different application domains. However, recent studies have shown that implementation errors, nonce reuse, improper initialization vector (IV) generation, and incorrect authentication procedures remain significant causes of security failures even when strong block ciphers such as AES are used. Consequently, recent research has shifted from evaluating block ciphers alone to examining the security properties and deployment requirements of their associated modes of operation.

➢ *Studies on CPA-Secure Encryption Modes*

Several researchers have investigated the confidentiality guarantees provided by CPA-secure block cipher modes. Modes such as CBC and CTR remain computationally efficient and achieve indistinguishability under chosen-plaintext attacks when correctly implemented with unpredictable initialization vectors or unique nonces. Nevertheless, recent analyses emphasize that confidentiality alone is insufficient for modern network environments because CPA-secure encryption does not inherently provide message integrity or protection against active adversaries capable of manipulating ciphertexts. These findings reinforce the importance of combining confidentiality with authentication in practical cryptographic systems.

Performance evaluations conducted on contemporary AES modes similarly indicate that authenticated encryption modes such as GCM provide stronger overall security than traditional confidentiality-only modes while maintaining high computational efficiency, making them more suitable for current communication protocols.

➢ *Research on Authenticated Encryption and CCA Security*

Authenticated Encryption (AE) has become one of the most active research areas in modern cryptography because it simultaneously guarantees confidentiality and message integrity. Jimale et al. (2022), in a comprehensive systematic review published in IEEE Access, classified authenticated encryption schemes according to their design approaches, security properties, efficiency, and implementation characteristics. Their review concluded that although numerous authenticated encryption schemes have been proposed, balancing strong security, computational efficiency, and practical implementation remains an important research challenge.

Similarly, recent discussions within the NIST cryptographic community highlight the continued importance of AES-GCM while identifying practical challenges associated with nonce management, authentication-tag requirements, and large-scale cloud deployments (Kampanakis et al., 2024). These studies recommend strengthening authenticated encryption standards to improve robustness against misuse and implementation errors while preserving high performance in modern distributed systems.

➢ *Research Gap*

The reviewed literature demonstrates substantial progress in the development of secure block ciphers, block cipher modes of operation, and authenticated encryption schemes. Existing studies have extensively examined these topics independently by focusing on AES security, authenticated encryption, implementation efficiency, or standardized cryptographic modes. However, relatively few studies present a unified discussion explaining how cryptographic security progresses from pseudorandom permutations through CPA-secure block cipher modes to CCA-secure authenticated encryption within a single conceptual framework.

Therefore, this study addresses this gap by providing an integrated review that connects the theoretical foundations of pseudorandom permutations with the practical security properties of block cipher modes of operation and authenticated encryption. The study demonstrates how these interconnected concepts collectively contribute to achieving confidentiality, integrity, and resistance against chosen-ciphertext attacks in modern secure communication systems.

III. METHODOLOGY

➢ *Research Design*

This study adopts a structured literature review design, consistent with its aim of examining how cryptographic security progresses from pseudorandom permutations through CPA-secure modes of operation to CCA-secure authenticated encryption within a single conceptual framework. A review design was selected over an experimental or simulation-based design because the study's contribution is the synthesis and integration of established theoretical and empirical findings across three normally separate bodies of literature block cipher theory, mode-of-operation security analysis, and authenticated encryption research rather than the generation of new cryptanalytic or performance results.

➢ *Sources of Data and Search Strategy*

Data for this review were drawn from peer-reviewed journals, NIST publications and standardization reports, IEEE and ACM conference proceedings, and the IACR Cryptology ePrint Archive. Search terms included combinations of "pseudorandom permutation," "block cipher mode of operation," "chosen-plaintext attack," "chosen-ciphertext attack," and "authenticated encryption." Priority was given to sources published within the last five years to satisfy the currency requirements of a rapidly evolving field, while foundational theoretical sources establishing the core security definitions were retained regardless of publication date, since these remain the primary references for the proofs the study relies on.

➢ *Review Method Aligned to Each Objective*

To ensure that every objective is addressed by a distinct and traceable method, the following four review methods were applied:

- Objective i – Examine the role of pseudorandom permutations in the construction of secure block ciphers.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

This objective was addressed through conceptual/definitional analysis: the formal definitions of pseudorandom functions (PRFs) and pseudorandom permutations (PRPs) were drawn from foundational cryptographic theory and cross-referenced against current assessments of AES as a practical realization of the PRP abstraction (NIST, 2023), to establish the theoretical basis on which the rest of the review depends.

- Objective ii – Analyze the security properties of major block cipher modes of operation under chosen-plaintext attacks. This objective was addressed through comparative mode analysis: each major mode of operation (CBC, CTR, CFB, OFB, GCM) was examined against the formal requirements for IND-CPA security, drawing on recent evaluations of mode-level security and implementation practice (Mouha & Dworkin, 2024), to classify each mode's CPA status and identify the specific implementation factors (IV predictability, nonce reuse) that determine whether that status holds in practice.
- Objective iii – Investigate the limitations of CPA-secure encryption and the security requirements of chosen-ciphertext attack resistance. This objective was addressed through gap analysis of documented vulnerabilities: literature on padding-oracle attacks, nonce misuse, and ciphertext-manipulation exploits was reviewed to identify the specific conditions under which CPA-secure modes fail against active adversaries, establishing the formal requirements that IND-CCA security must additionally satisfy.
- Objective iv – Evaluate authenticated encryption techniques used to achieve confidentiality, integrity, and authentication in modern cryptographic protocols. This objective was addressed through comparative evaluation of authenticated encryption schemes: systematic classifications of authenticated encryption approaches (Jimale et al., 2022) were reviewed alongside current NIST guidance on AES-GCM deployment challenges (Kampanakis et al., 2024) and lightweight AEAD standardization outcomes (Kaur et al., 2023), to evaluate how current schemes balance security guarantees against implementation and performance constraints in deployed systems.

➢ *Limitations of the Method*

As a literature-based review rather than an experimental study, this research does not produce new cryptanalytic results, formal proofs, or performance benchmarks; its contribution lies in synthesizing existing findings into an integrated framework. Because the review is narrative rather than systematic in the PRISMA sense (Page et al., 2021), source selection while guided by the criteria in Section 3.2 retains an element of researcher judgment regarding relevance and depth of coverage.

IV. RESULTS AND DISCUSSION

➢ *Pseudorandom Permutations as the Foundation of Secure Block Ciphers*

The reviewed literature consistently identifies pseudorandom permutations (PRPs) as the theoretical foundation upon which modern block ciphers are constructed. A PRP is a keyed permutation that is computationally indistinguishable from a truly random permutation to any efficient adversary without knowledge of the secret key. This property enables block ciphers to transform plaintext into ciphertext while maintaining computational unpredictability under accepted security assumptions (Katz & Lindell, 2020). This formalization traces back to the foundational treatment of probabilistic and semantic security introduced by Goldwasser and Micali (1984), later extended into a concrete security framework for symmetric encryption by Bellare, Desai, Jokipii, and Rogaway (1997), which underlies the reduction-based proofs discussed throughout this review.

Formally, let $F: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a keyed function family. F is a pseudorandom function (PRF) if, for every efficient (probabilistic polynomial-time) adversary A with oracle access, the following distinguishing advantage is negligible in n:

$$Adv^{PRF}(A) = | Pr[K \leftarrow \{0,1\}^k : A^{\{F_k(\cdot)\}} = 1] - Pr[f \leftarrow Funcs[n] : A^{\{f(\cdot)\}} = 1] | \leq negl(n)$$

F is additionally a pseudorandom permutation (PRP) if F_k is a bijection on $\{0,1\}^n$ for every key K, and the adversary's task is to distinguish $F_k(\cdot)$ from a uniformly random permutation $\pi \leftarrow$ Perms[n] rather than from a random function. Because every PRP is trivially a permutation, it can never be perfectly indistinguishable from a random function; the PRP/PRF switching lemma bounds this statistical distance for q oracle queries as:

$$| Pr[A^{\{\pi(\cdot)\}} = 1] - Pr[A^{\{f(\cdot)\}} = 1] | \leq q^2 / 2^{n+1}$$

This “birthday bound” is the formal reason why block length, and not merely key length, is a security-relevant design parameter: for a 64-bit block cipher, the bound becomes non-negligible once q approaches 2^{32} queries a volume reachable in high-traffic network settings whereas AES's 128-bit block pushes the same bound out to $q \approx 2^{64}$, currently infeasible.

Recent evaluations by the National Institute of Standards and Technology (NIST) continue to recognize the Advanced Encryption Standard (AES) as the benchmark realization of the PRP model. According to NIST (2023), no practical cryptanalytic attacks capable of compromising the complete AES algorithm have been demonstrated despite more than two decades of extensive public analysis. This continued confidence reinforces the role of AES as the preferred symmetric-key primitive for protecting sensitive information across government, financial, healthcare, and commercial applications.

The reviewed studies further distinguish between provable security and assumed security. While the security of encryption modes can often be formally reduced to the assumption that the underlying block cipher behaves as a secure PRP, the block cipher itself cannot generally be proven secure from a mathematical hardness assumption. Instead, confidence in AES derives from continuous public cryptanalysis and practical resistance against differential,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

linear, algebraic, and related-key attacks (Mouha & Dworkin, 2024). Consequently, the effectiveness of higher-level encryption schemes depends fundamentally on the strength of the underlying PRP.

These findings demonstrate that pseudorandom permutations provide the theoretical basis upon which modern symmetric encryption is built, thereby satisfying the first objective of this study.

- *Security Analysis of Block Cipher Modes under Chosen-Plaintext Attacks*

The reviewed literature shows that block ciphers alone cannot securely encrypt messages of arbitrary length and therefore require modes of operation to provide practical encryption. Commonly deployed modes include Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR), and Galois/Counter Mode (GCM), each possessing distinct security characteristics and implementation requirements (Mouha & Dworkin, 2024).

Among these modes, ECB remains unsuitable for secure communication because identical plaintext blocks always produce identical ciphertext blocks, resulting in observable data patterns. Consequently, ECB fails to satisfy indistinguishability under chosen-plaintext attacks (IND-CPA) and is generally discouraged for practical applications.

In contrast, CBC, CFB, OFB, and CTR achieve CPA security when implemented with unpredictable initialization vectors or unique nonces. The reviewed literature consistently emphasizes that these security guarantees depend on correct implementation rather than the encryption mode alone. Predictable initialization vectors, repeated nonces, or poor key management may significantly weaken otherwise secure encryption systems.

Recent evaluations further indicate that authenticated encryption modes such as AES-GCM provide confidentiality while simultaneously incorporating integrity protection, thereby reducing implementation complexity compared with traditional combinations of encryption and message authentication. Because of these advantages, GCM has become the preferred encryption mode for Transport Layer Security (TLS), cloud services, and many contemporary communication protocols (Kampanakis et al., 2024).

Table 1 summarizes the CPA-security status of each mode alongside its principal weakness, drawn from the comparative mode analysis described in Section 3.3:

Table 1: CPA-Security Status and Principal Weakness of Common Modes of Operation

Mode of Operation	IND-CPA Secure?	Principal Weakness
Electronic Codebook (ECB)	No	Deterministic per block; identical plaintext blocks yield identical ciphertext blocks, leaking patterns
Cipher Block Chaining (CBC)	Yes, with a random, unpredictable IV	Malleable; vulnerable to padding-oracle attacks and predictable-IV exploits (e.g., BEAST) under CCA
Cipher Feedback (CFB)	Yes, with a random IV	Malleable; susceptible to bit-flipping attacks
Output Feedback (OFB)	Yes, with a random IV	Catastrophic failure if keystream is reused
Counter (CTR)	Yes, if counter/nonce never repeats under the same key	Nonce reuse is catastrophic (two-time-pad problem); ciphertext fully malleable
AES-GCM (AEAD)	Yes, and additionally IND-CCA secure	Security collapses completely under nonce reuse; otherwise integrates authentication natively

Figure 1 visualizes the same comparison in terms of the three security properties examined throughout this review confidentiality under IND-CPA, message integrity, and IND-CCA resistance making explicit that only an integrated AEAD construction satisfies all three simultaneously.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

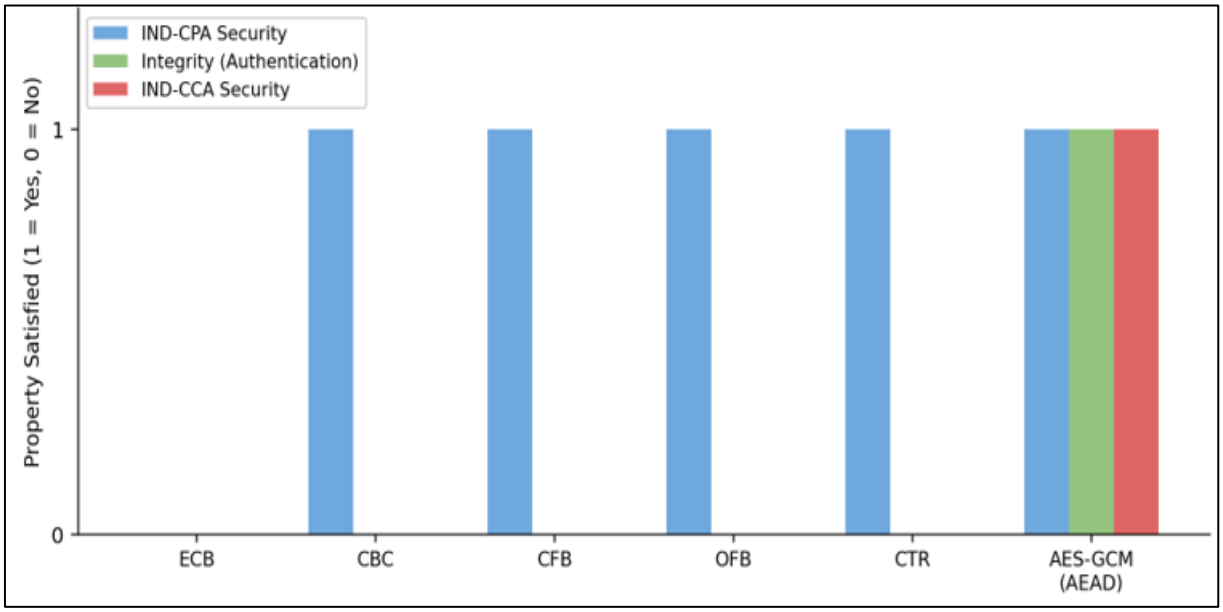

Fig 1: Security Properties Satisfied by Block Cipher Modes of Operation

Overall, the reviewed evidence confirms that the practical security of block cipher modes depends equally on cryptographic design and implementation practices, thereby addressing the second objective of this study.

➢ *Limitations of CPA Security and the Need for Chosen-Ciphertext Security*

Although CPA-secure encryption provides strong confidentiality against passive adversaries, the reviewed literature demonstrates that it offers insufficient protection in environments where attackers can actively manipulate ciphertexts. Modern communication systems frequently expose decryption mechanisms through network protocols, error handling, timing information, or application responses, thereby enabling chosen-ciphertext attacks.

The two adversarial models reviewed can be stated formally as indistinguishability games. In the IND-CPA game, the challenger samples $K \leftarrow \{0,1\}^k$, grants the adversary A oracle access to $Enc_k(\cdot)$, and upon receiving two equal-length messages m_0, m_1 from A, returns a challenge ciphertext $c^* = Enc_k(m\_b)$ for a randomly chosen bit $b \leftarrow \{0,1\}$. The scheme is IND-CPA secure if:

$$Adv^{ONA}(A) = | Pr[A(c^*) = b] - ½ | \leq negl(n)$$

The IND-CCA game strengthens this model by additionally granting A oracle access to decryption, $Dec_k(\cdot)$, both before and after receiving the challenge ciphertext subject only to the restriction that A may not query $Dec_k(c^*)$ directly. A scheme is IND-CCA secure if $Adv^{ONccA}(A)$ remains negligible even against this strictly more powerful adversary.

Several documented attacks illustrate these weaknesses. Padding-oracle attacks exploit differences in system responses during padding verification to recover plaintext without knowledge of the encryption key (Vaudenay, 2002). Krawczyk (2001) demonstrated that the composition order of encryption and authentication is not immaterial: MAC-then-Encrypt, as historically used in SSL/TLS, does not generically guarantee CCA security, providing an early theoretical account of the vulnerability class that padding-oracle attacks later exploited in practice. Similarly, nonce reuse in stream-based encryption modes such as CTR and GCM may result in catastrophic confidentiality failures by allowing attackers to derive relationships between encrypted messages. These findings confirm that confidentiality alone cannot adequately secure modern communication systems.

Recent literature therefore emphasizes that cryptographic systems must satisfy both confidentiality and integrity requirements. The chosen-ciphertext attack (IND-CCA) security model extends CPA security by assuming that attackers may obtain decryption results for carefully selected ciphertexts, except for the challenge ciphertext itself. Encryption schemes that remain secure under this stronger adversarial model provide substantially greater practical protection than confidentiality-only constructions (Jimale et al., 2022).

The reviewed evidence therefore establishes that CPA security should be regarded as a necessary but insufficient security requirement, thereby supporting the third objective of this study.

➢ *Evaluation of Authenticated Encryption Techniques*

The reviewed literature consistently identifies authenticated encryption as the current best practice for securing modern communication systems. Authenticated Encryption with Associated Data (AEAD) combines encryption and authentication into a unified cryptographic primitive that simultaneously provides confidentiality, integrity, authenticity, and resistance against chosen-ciphertext attacks. The theoretical basis for this convergence traces to Bellare and Namprempre (2000), who proved that Encrypt-then-MAC generically achieves CCA security regardless of the underlying primitives, and to Rogaway

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

(2011), whose evaluation of blockcipher modes of operation helped establish integrated AEAD constructions as the preferred alternative to manual composition.

Among the authenticated encryption schemes examined, AES-GCM remains the most widely deployed because of its computational efficiency, support for hardware acceleration, and compatibility with modern communication protocols. However, recent studies caution that the security of AES-GCM depends heavily on correct nonce management. Reusing a nonce under the same encryption key may completely compromise confidentiality and authentication guarantees, highlighting the importance of secure implementation practices (Kampanakis et al., 2024).

The literature also recognizes ChaCha20-Poly1305 as an efficient alternative to AES-GCM, particularly for resource-constrained environments and software-based implementations where dedicated AES hardware acceleration is unavailable. Furthermore, recent lightweight cryptography initiatives by NIST have encouraged the development of authenticated encryption algorithms suitable for Internet of Things (IoT) devices with limited computational resources (Kaur et al., 2023).

More recent research has identified security properties beyond classical IND-CCA that AEAD schemes must satisfy in practice. Albertini et al. (2022) demonstrate that AEAD schemes lacking key-commitment can be abused in multi-recipient and password-based settings, while Inoue (2022) extends AEAD security proofs beyond fixed input-length limitations. These findings indicate that AEAD security remains an active and evolving research area rather than a settled endpoint, reinforcing the value of situating this review's classical CPA/CCA framework within current, ongoing research.

Overall, the reviewed studies conclude that authenticated encryption provides the most comprehensive security framework for modern symmetric cryptography because it effectively addresses the confidentiality and integrity requirements demanded by contemporary communication systems. These findings satisfy the fourth objective of this study.

➢ *Discussion of Findings*

Figure 2 synthesizes the findings of Sections 4.1–4.4 into a single visual argument: security propagates from an assumed-secure block cipher, through a formally CPA-secure mode of operation, to a deployment-ready CCA-secure construction achieved either by composing a CPA-secure mode with an independent MAC, or by adopting an integrated AEAD scheme directly.

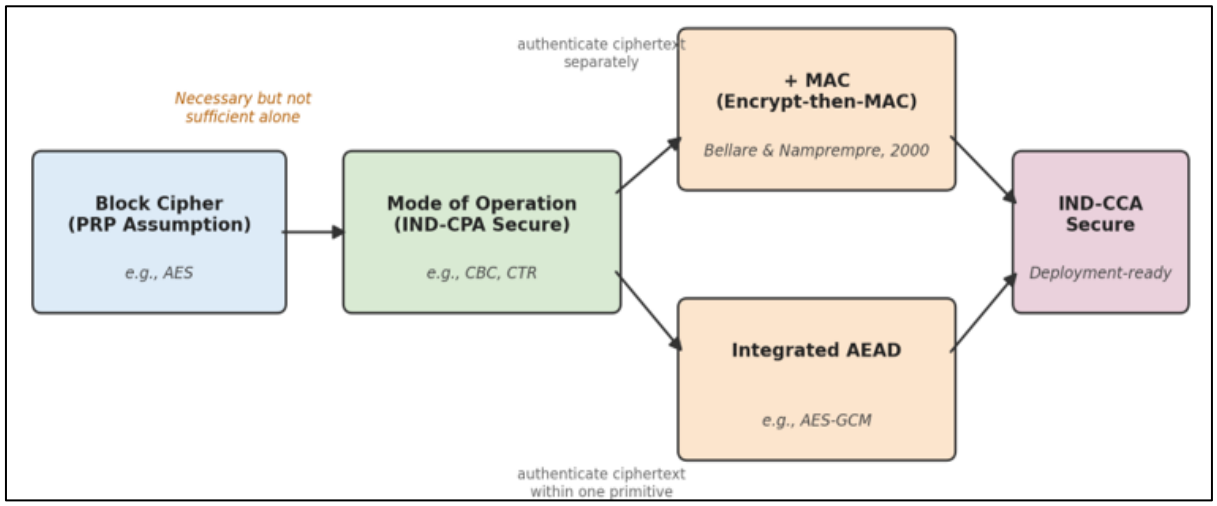

Fig 2: Layered Propagation of Symmetric-Key Encryption Security

The findings of this review demonstrate a clear progression in the development of modern symmetric-key cryptography. Security begins with the assumption that a block cipher behaves as a secure pseudorandom permutation, extends through carefully designed block cipher modes that achieve confidentiality under chosen-plaintext attacks, and culminates in authenticated encryption schemes capable of resisting active adversaries through chosen-ciphertext security.

Unlike many previous studies that discuss these concepts independently, this review integrates pseudorandom permutations, CPA-secure modes, chosen-ciphertext security, and authenticated encryption into a single conceptual framework. The synthesis demonstrates that practical cryptographic security depends not only on strong algorithms but also on correct implementation, authenticated encryption, secure nonce management, and adherence to established cryptographic standards.

The reviewed literature therefore supports the widespread recommendation that authenticated encryption, particularly standardized AEAD schemes such as AES-GCM and ChaCha20-Poly1305, should serve as the default approach for securing modern communication systems.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

V. CONCLUSION

This study examined the progression of security in modern symmetric-key cryptography from pseudorandom permutations (PRPs) and block ciphers through chosen-plaintext attack (CPA)-secure modes of operation to chosen-ciphertext attack (CCA)-secure authenticated encryption schemes. The study was motivated by the need to provide an integrated understanding of these interconnected concepts, which are often discussed separately in the existing literature despite their collective importance in the design of secure communication systems.

The review established that pseudorandom permutations provide the theoretical foundation upon which modern block ciphers, particularly the Advanced Encryption Standard (AES), are constructed. Furthermore, the study found that while block cipher modes such as CBC and CTR achieve confidentiality under the CPA security model when correctly implemented, they remain vulnerable to active attacks in environments where ciphertext manipulation is possible. Consequently, confidentiality alone is insufficient for protecting modern communication systems.

The findings further demonstrated that authenticated encryption techniques, especially Encrypt-then-MAC constructions and Authenticated Encryption with Associated Data (AEAD) schemes such as AES-GCM and ChaCha20-Poly1305, provide stronger security guarantees by simultaneously ensuring confidentiality, integrity, and authenticity while resisting chosen-ciphertext attacks. These findings reinforce current cryptographic recommendations that authenticated encryption should serve as the default approach for securing contemporary communication protocols.

A major contribution of this study is the integration of pseudorandom permutations, block cipher modes of operation, CPA security, and CCA-secure authenticated encryption into a unified conceptual framework. By synthesizing theoretical foundations with recent developments in cryptographic standards and implementation practices, the study provides a clearer understanding of how secure symmetric-key encryption is achieved in practical systems.

Future research should investigate the security implications of authenticated encryption in emerging computing environments, including Internet of Things (IoT) devices, cloud-native architectures, post-quantum cryptographic systems, and resource-constrained embedded platforms. Additional studies may also evaluate the performance, scalability, and implementation challenges of newly standardized lightweight authenticated encryption algorithms in real-world deployments.

REFERENCES

[1]. Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., & Schmieg, S. (2022). How to abuse and fix authenticated encryption without key commitment. In Proceedings of the 31st USENIX Security Symposium (pp. 3291–3308). USENIX Association.

[2]. Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997). A concrete security treatment of symmetric encryption. Proceedings of the 38th Annual Symposium on Foundations of Computer Science, 394–403.

[3]. Bellare, M., & Namprempre, C. (2000). Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto (Ed.), Advances in Cryptology – ASIACRYPT 2000 (Lecture Notes in Computer Science, Vol. 1976, pp. 531–545). Springer.

[4]. Dworkin, M. J. (2001). Recommendation for block cipher modes of operation: Methods and techniques (NIST Special Publication 800-38A). National Institute of Standards and Technology.

[5]. Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 28(2), 270–299.

[6]. Inoue, A. (2022). Beyond full-bit secure authenticated encryption without input-length limitation. IET Information Security, 16(4), 253–261.

[7]. Jimale, M. A., Z'aba, M. R., Kiah, M. L. B. M., Idris, M. Y. I., Jamil, N., Mohamad, M. S., & Rohmad, M. S. (2022). Authenticated encryption schemes: A systematic review. IEEE Access, 10, 14739–14766.

[8]. Kampanakis, P., Campagna, M., Crocket, E., Petcher, A., & Gueron, S. (2024). Practical challenges with AES-GCM and the need for a new cipher. In Proceedings of the Third NIST Workshop on Block Cipher Modes of Operation. National Institute of Standards and Technology.

[9]. Katz, J., & Lindell, Y. (2020). Introduction to modern cryptography (3rd ed.). CRC Press.

[10]. Kaur, J., Cintas Canto, A., Mozaffari Kermani, M., & Azarderakhsh, R. (2023). A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. ACM Computing Surveys.

[11]. Krawczyk, H. (2001). The order of encryption and authentication for protecting communications (or: How secure is SSL?). In J. Kilian (Ed.), Advances in Cryptology – CRYPTO 2001 (Lecture Notes in Computer Science, Vol. 2139, pp. 310–331). Springer.

[12]. Mouha, N. (2021). Review of the Advanced Encryption Standard (NIST Interagency/Internal Report 8319). National Institute of Standards and Technology.

[13]. Mouha, N., & Dworkin, M. (2024). Report on the block cipher modes of operation in the NIST SP 800-38 series (NIST Interagency/Internal Report 8459). National Institute of Standards and Technology.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1487

[14]. National Institute of Standards and Technology. (2023). Advanced Encryption Standard (AES) (FIPS Publication 197, Update 1). U.S. Department of Commerce.
[15]. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372, n71.
[16]. Rogaway, P. (2011). Evaluation of some blockcipher modes of operation. CRYPTREC. https://www.cryptrec.go.jp/en/
[17]. Vaudenay, S. (2002). Security flaws induced by CBC padding: Applications to SSL, IPSEC, WTLS. In L. R. Knudsen (Ed.), Advances in Cryptology – EUROCRYPT 2002 (Lecture Notes in Computer Science, Vol. 2332, pp. 534–545). Springer.