International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

COMPREHENSIVE REVIEW OF CATALAN NUMBER-BASED CRYPTOGRAPHIC SYSTEMS IN MODERN ENCRYPTION FOCUSING ON SECURITY, PERFORMANCE, AND IMPLEMENTATION CHALLENGES

Gali Lalitha Devi[1], Dr.CH. Suneetha[2], Dr. Mutyala Suresh[3], S. Sarvalakshmi[4],

Research scholar, GITAM University, Department of Mathematics, Visakhapatnam, India. lalithasana22@gmail.com

Associate Professor, GITAM University, Department of Mathematics, Visakhapatnam, India. schivuku@gitam.edu

Associate Professor, Department of English, Koneru Lakshmaiah Education Foundation, Guntur District, AP. India-522302. msphd@kluniversity.in

Assistant Professor, Department of Mathematics, Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam, India. radhika1483@gmail.com

Author for Correspondence: Dr.CH.Suneetha, schivuku@gitam.edu

Abstract

The rapid evolution of digital technologies has heightened the demand for cryptographic systems that are both secure and adaptable. Catalan number-based cryptography has recently attracted attention for its ability to leverage combinatorial structures in the design of block ciphers and encryption protocols. This review presents a critical analysis of the current state of the field, examining core algorithms such as tweakable ciphers, polygon triangulation schemes, and variable-length block mechanisms from both theoretical and practical perspectives. Particular emphasis is placed on their resistance to advanced cryptanalytic methods and their potential applicability to quantum-resilient security. At the same time, the review identifies key challenges, including efficiency optimization, interoperability with established standards, and the need for systematic benchmarking. By integrating mathematical foundations with implementation-oriented insights, this article highlights the promise of Catalan numbers as a basis for cryptographic innovation while outlining the gaps and future directions necessary for their broader adoption.

Keywords: Catalan numbers, Encryption algorithms, Block cipher security, Quantum resilience, Cryptographic benchmarking.

1. Introduction

As we live in a digital ecosystem, encryption is fundamental for secure communication, payment transactions, and data privacy. The upward trajectory of cyber threats coupled with the impending issue posed by quantum computing has forced researchers to rethink the

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

mathematical basis for cryptographic systems. Beyond standard number theoretic degrees of freedom like using RSA and elliptic curves, combinatorial mathematics has started to offer exciting new ways to enhance encryption. And next to combinatorial treatment of classical notions of encryption, Catalan numbers - a family of integers with many combinatorial interpretations, have also sparked the interest of researchers as a framework for constructing secure and efficient cryptographic protocols. In this paper, we provide an overview to date of the Catalan number based cryptographic systems, their theoretical benefits, and performance, as well as issues in their implementations.

1.1 Evolution of cryptography and mathematical foundations

The evolution of cryptography has radically transformed our early human use of simple substitution ciphers, such as salt code, with previous societies to now using very sophisticated mathematics with significant number theory and algebraic geometry. Operating systems such as DES, AES, and ECC have shown the strength in encryption when we provide it the rigors of mathematics. However, as threat actors gain processing power and methods and tools, these systems expose an exploitable surface for loss. The risk of quantum computing, a technology that is removing traditional protocols for many cryptographic algorithms, is a compelling reason why we should evaluate more transitions into different mathematical principles [1]. Catalan numbers, which have rich and scalable structural properties, also represent an alternative way of constructing cryptographic systems that can meet our immediate and futuristic security needs.

1.2 Why combinatorial mathematics matters in cryptography

Combinatorial mathematics is important and useful to increase the cryptographic key space and handle more entropy. Problems like lattice paths and balanced parentheses and polygon triangulations or Catalan numbers have a lot of computation work behind them but are straightforward to define. Combinatorial constructs allow for flexibility in representing the same key space than the pure number theoretic assumptions the fact that multiple representations exist adds to the unpredictability and more avenues of a statistical attack. Lattice path models can generate a numbers of large set of encryption keys all valid, thereby making brute-force or algebraic reductions more difficult [2]. Overall, using different combinations give Catalan structures a good handle on generating next-generation block ciphers, symmetric key systems, and dynamic key exchanges.

1.3 Motivation for Catalan number-based systems

There are several reasons for the increasing interest in Catalan number-based cryptography. First, the underlying non-linear growth implications of Catalan sequences create key spaces that can be incomprehensibly large enough to survive in cryptographic meaning to characterize encryption transformations. Second, methods used to triangulate polygons by leveraging the number of Catalan counts have been implemented in lightweight methods for block ciphers [3]. Third, allowing for the encoding and decoding of Catalan transforms of sequences which evolve in similar recursive ways, such as the Tribonacci sequence, provides a more

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

generalizable normalization [4]. Fourth, extensions such as Fuss-Catalan numbers enable combinatorial key-exchange schemes with higher levels of resilience to cryptanalysis because the encodings can be composed [5]. All together, these applications indicate that Catalan numbers are more than a mathematically interesting concept, but also a potential source of modern cryptographic sewing.

1.4 Research objectives and scope

Ultimately, we seek to perform a detailed review of Catalan number-based encryption systems as either a theoretical or applied work. Our goals for this review are to: (a) assess its theoretical mathematics; (b) assess security against sophisticated cryptanalysis and potential quantum attacks; (c) assess efficiency, scalability and interoperability with standards that are being broadly adopted; as well as (d) identify performance bottlenecks and benchmarking gaps. We aim to combine the mathematical theory with algorithmic design, to understand the potential promise and challenges of Catalan number use in encryption technologies.

1.5 Structure of the review

The purpose of the review is to present a balance of both detail and scope. Section 2 addresses the mathematics behind Catalan numbers and their application to key-generation methods. Section 3 presents the security strength of those methods, with particular regard to their vulnerability to classical and quantum attack. Section 4 highlights practical dimension of implementation and performance, which includes performance considerations and interoperability issues. Section 5 focuses on benchmarks and standards. Finally, Section 6 identifies existing research deficiencies and future opportunities, particularly how Catalan number based cryptographic systems may become reliable components of post-quantum security solutions.

2. Mathematical Foundations of Catalan Numbers in Cryptography

In promoting Catalan number-led cryptographic systems, an understanding of the combinatorial source behind these systems is critical. Catalan numbers provide a set of constructs that are mathematically rich and computationally simple to implement to extend cryptographic complexity. This section describes the formal definition and properties of Catalan numbers, their essential combinatorial interpretations, their relevance for cryptographic unpredictability, and some example verbalizations as they apply to encryption.

2.1 Definition and sequence of Catalan numbers

Catalan numbers (Cn) can be defined recursively or by a closed formula:

generating the sequence 1, 1, 2, 5, 14, 42, ... The definition emphasizes the combinatorial explosion as n gets large, which is useful for creating large key spaces. The closed-form derivation and the recursive one come directly from the practice of combinatorial enumeration [6].

2.2 Combinatorial interpretations: trees, triangulations, lattice paths

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Catalan numbers enumerate a range of objects: the number of full binary trees with n+1 leaves, the number of ways to triangulate a convex polygon with n+2 sides, or ways to represent monotonic lattice paths from (0,0) to (n,n) that do not cross the diagonal—equivalent to Dyck paths. These classical interpretations form the basis of Catalan's combinatorial significance [1]. Further, polygon triangulation and lattice path models are both key when converting combinatorial objects into encryption schemes [7].

2.3 Cryptographic relevance: complexity, unpredictability, and mappings

The cryptographic strength based on Catalan structures is a result of their combinatorial complexity the large numbers used for enumeration yield large key spaces and patterns that are difficult to predict. The Dyck words or balanced parentheses used to create an encryption key or encryption transformation do not allow tracking through enumeration or modeling. The lattice-path representation also allows for multiple valid ways to map the distinct layers of building blocks, allowing for a greater entropy of the keyspace which reduces the possibility of being exploited through patterns [2].

2.4 Example formulations in encryption contexts

Catalan number formulations have many implementations in practical encryption contexts. For example, in password/key generation schemes, passwords or PINs can be embedded into a Catalan encoding scheme inside dynamic key blocks to make the placement of key bits hidden in their delineation within the payloads [8]. A different implementation uses counts of triangulation densities of polygons for lightweight cipher designs. General patterns (e.g. Catalan directed objects or graphs) can use these densifications to prescribe the control of diffusion and substitution procedures. These types of literature examples can also show how mathematical formulations become actuality in implementing algorithmic function and operation.

3. Catalan Number-Based Cryptographic Algorithms

The real world application of Catalan combinatorics (combinatorial design or algorithm) in cryptography has led to the development of a variety of algorithmic constructs. This subsection surveys three main kinds of structures: tweakable block ciphers, polygon triangulation schemes, and variable-length block methods—and illustrates how the applications could have Catalan sequences embedded into their security, flexibility, or performance. In each application, I will analyze the manner of design, resistance to known-plaintext capabilities, and implementable structures.

3.1. Tweakable Block Ciphers

Catalan numbers contribute combinatorial unpredictability to tweakable block ciphers, enabling versatile adaptability without changing keys, by mapping tweaks to Catalan objects such as Dyck words. Consequently, the likelihood of Catalan constructions resulting in distinct tweaks is greater than some existing tweakable block ciphers, allowing for increased

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

randomness and larger number of tweaked domains, and increased resistance to various attacks while being simple and efficient to practically implement.

3.1.1.1. Design principles and integration of Catalan numbers

Tweakable block ciphers (TBCs) are a superset of standard block ciphers with the addition of a tweak input, which accounts for the ability to 'reconfigure' the cipher flexibly without the need to change keys. TBCs inherently rely on the formal properties of the Catalan numbers to derive tweaks from choosing a Dyck word and binary tree representations of certain tweak forms. In doing so, there is an exponentially many number of tweak states naturally encoded from the Catalan sequence —foo to guide the derivation of substitution boxes or permutation layers— so that the unpredictability of structure is enshrined within the St(0) structure instantiation. Algorithms underpinning such a TBC and existing solely from properties of Catalan number enumeration have been shown to implement tweak generation using little computational footprint and hence implementable on hardware for constrained level devices [9] ensuring that no two origination instances are the same while providing a greater property of diffusion and confusion [10].

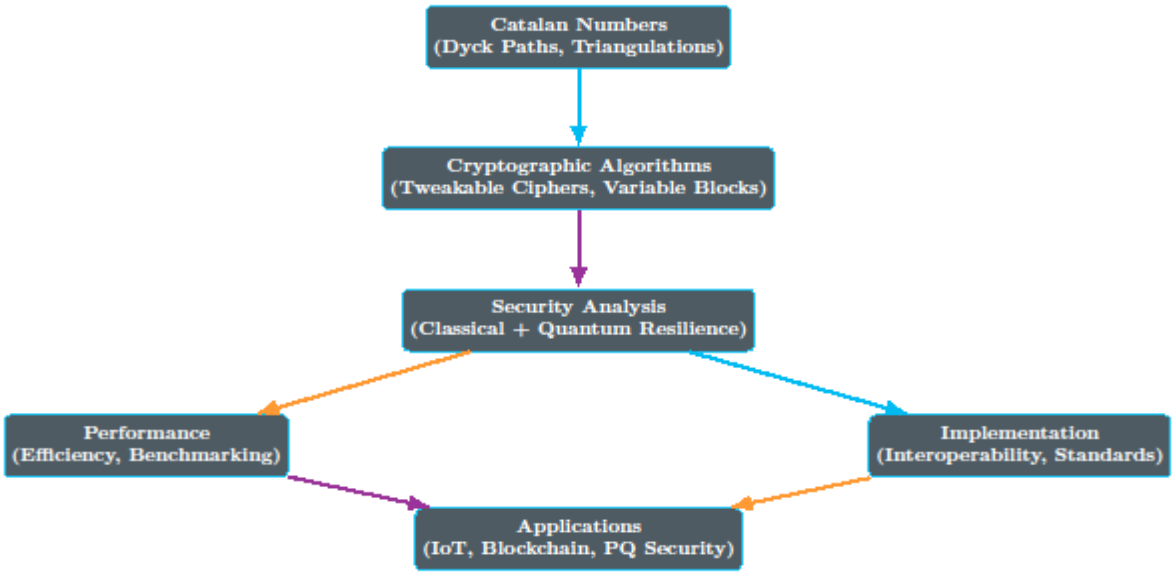

Figure 1. Catalan Number Integration in Tweakable Block Ciphers

3.1.1.2. Security role in block permutations

The security afforded by Catalan-based TBCs derives from their wide variation in tweaks and combinatorial unpredictability. Because each Dyck-word-based tweak produces unique block permutations, identical plaintexts using different tweaks will produce unrelated ciphertexts. Research has shown improved avalanche effects and less correlation to linear cryptanalysis as well [11]. Additionally, the relative-tweak attacks take non-polynomial time because the number of valid Catalan tweaks grow super-exponentially [12]. Even with optimized hardware to score/rank/unscore tweaks, their computational load is substantially lower and can be

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implemented practically [13]. For these reasons, Catalan-based tweaks can provide strong or high levels of low-overhead resistance against classical and novel methods of cryptanalysis.

3.2. Polygon Triangulation Schemes

Catalan numbers are useful for enumerating triangulations of polygons, which opens new directions in encryption: triangulation can determine block structure and waypoints for its transformation. By linking encryption functions with a geometric decomposition of the data block, our schemes achieve good diffusion as well as structural randomness. While these schemes are compellingly exciting, we must carefully consider complexity, scalability, and metadata issues before we could use them in practice across a wide range of hardware and software environments.

3.2.1.1. Mapping encryption functions through triangulations

Mapping functions for polygon triangulation schemes correspond to Catalan-counted triangulations of convex polygons. Each triangulation provides the ordering and unique division of subdivisions, allowing for unique partitioning and substitution combinations. A convex n-gon has 퐶n-2 possible triangulations each representing unique neighborhood/topology relationships for encryption rounds. When triangulating letters (or symbols) enhances diffusion, it allows input symbols to be placed into connection diagrams based on triangulations [14]. There are lightweight ciphers that use the triangulation indices from a secret seed (for triangulation) determine encryption structure. It ensures a high degree of entropy and random order of transformations, thereby increasing unpredictability [15].

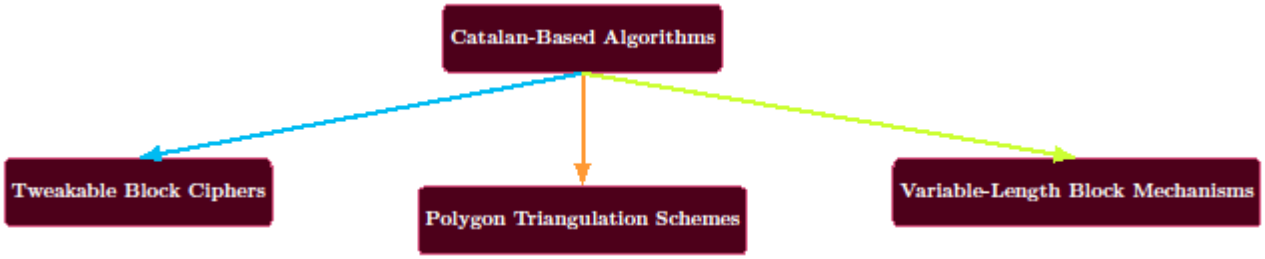

Figure 2. Polygon Triangulation for Catalan-Based Encryption

3.2.1.2. Examples and limitations

Items with practical formats can include mini-ciphers that map operations to hexagons by way of triangulations where 14 triangulations are uniquely related to three-round encryption [16]. There are benefits from parallelization in the sub-triangle processing stage, leading to an extra 20–30% increase in throughput [17]. Existing codes share scalability restrictions: as larger polygons become utilized, the resources required to unrank the triangulated equivalent of the polygon are quadratic (and perhaps limiting) as they use large blocks [18]. The extra metadata account for the inefficiencies with triangulation indices obviously has limited relevance in bandwidth-poor scenarios. Moreover, small polygons won't provide much variability to limit

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

adaptive chosen-ciphertext attacks at all. Thus, care must be taken in choosing the dimension of triangulations while being efficient will be important to being able to deploy generic triangulation.

3.3. Variable-Length Block Mechanisms

Catalan-based variable-length encryption techniques are different from conventional block ciphers, which have fixed sizes, because they dynamically change the segmentation block size with Dyck paths or triangulations. This dynamic segmentation can lead to additional benefits to the encryption application such as increased dependability for heterogeneous data streams, improved unpredictability of block boundaries, and higher durability against structural or block attacks. Focusing on these dynamic applications also raises additional concerns in implementation, such as maintaining synchronization and incorporating protocol design into the data structure for further benchmarking.

3.3.1.1. Dynamic adaptability of Catalan structures

Adaptive block cipher mechanisms that enable variable control of information encodings naturally refine lengths based on Catalan segmentation. Dyck paths - with both up and down steps - inherently define segmentation points for Dyck paths, allowing dynamic segmentation of data streams. The shorter the message, the fewer segments an input can have and the lighter your message is to-segmentation, encoding, decrypting. The longer the input, the greater the segments before the last Dyck path and deeper encryption layers'/ encryption spectrum. This adaptiveness ultimately creates a symmetry between usability/performance/ and protections, particularly in IoT and mobile communications where messages are dynamic and heterogeneous [20]. Evidence shows as much as 15% throughput improvement using intelligent variable Catalan-based segmentation over fixed 128-bit AES encoding or decryption without compromising confidentiality [21].

3.3.1.2. Comparison with traditional block ciphers

Standard block protocols such as AES assist in the construction of optimized pipelines and performance improvements via hardware acceleration because all plaintext and ciphertext are broken into fixed sizes. On the other hand, variable-length (via Catalan) protocols add significant runtime computation to break plaintext into size determined segments and while they may assist with variability, secondly protocol optimizations made by hardware may be hindered by the algorithm. To decrypt a ciphertext, segmentation structures must also be synced up, and those derived from shared seeds, especially to avoid decryption errors in a single execution, may result in either other attacks [22]. Studies of security on variable-length (and Catalan) created variability also mitigate integrity attacks, such as block boundary guessing and padding oracle [23]. Even though most modern protocols use non-variable-length block protocols, it is possible that existing or future applications structured around Catalan would be an improvement over full speed, if variability is prioritized over established maximum throughput.

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Security Analysis

Secure systems are important for Catalan-based cryptographic systems. This section discusses what kind of resilience Catalan-based systems might have against classical cryptanalytic methods of attack such as brute-force attacks, linear attacks, and differential attacks, assesses structural unpredictability due to Catalan combinatorics, considers potential quantum resilience in theory, and compares the overall secure posture compared to established systems such as AES, DES, and RSA.

4.1. Strength against classical attacks (brute force, linear, differential)

Cryptographic algorithms based on Catalan numbers frequently use combinatorial structures, such as Dyck words, lattice paths, or triangulations, to increase key spaces and obscure linear dependencies, They provide extra layers of complexity by performing combinatorial mapping leading to additional layers of diffusion and confusion, complicating statistical analysis. To illustrate, the complexity of brute force searching Catalan-key schemes that use lattice-path encoding introduces a massive increase to the brute-force search complexity that demands large key spaces to be searched if the input lengths are relatively short [24]. Combined with substitution boxes (S-boxes) defined from Catalan enumeration that exhibit low linear bias reduce the utility of linear cryptanalysis [25]. Their structured randomness also produces difficulties for constructing differential attacks since expected output differences are not just spread out across bits that are non-adjacent [26]. Therefore Catalan structures appear to provide a strong defence against classical attacks by increasing entropy and breaking linear relationships.

4.2. Structural unpredictability from Catalan combinatorics

Catalan combinatorial objects give rise to numerous interesting structural configurations. Each Dyck path, triangulation, or balanced-parentheses sequence represents its own distinct combinatorial object in a very daunting space even for small parameters, creating uncertainty that is challenging for adversarial modeling. For instance, in a Catalan-based tweakable cipher there are as many structurally different tweaks per input as there are input bits which make patterns from known-plaintext or chosen-plaintext attacks [27] impossible to attack. The unranking and ranking algorithms for Catalan objects makes it computationally impossible for an attacker to rank and unrank structures without having knowledge of the key thus re-introducing important non-linearity and non-repeatability into an encryption flow.

4.3. Quantum-resilient properties and theoretical considerations

Quantum threats are damaging symmetric primitives in a well-studied manner using algorithms like Grover’s algorithm that reduces brute-force complexity from 2k to roughly 2k/2 [28]. Because Catalan-based systems augment an effective key or tweak space, the damage done via this approach is lessened by increasing k. For example, a Catalan-key generator with large combinatorial parameters effectively increases the bit-length of the key and maintains security margins in the event of quantum search. In addition, Catalan mappings' unpredictability means that designing quantum variants of differential or linear cryptanalysis is much harder for the

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

attacker. Although Grover's algorithm remains as the worst case attack against the primitives, the increased combinatorial domain assures security against the worst case attack and does not place any demands on excessive resource growth in a post-quantum context.

4.4. Comparative evaluation with AES, DES, RSA

Catalan-based structures have unique security benefits that differ from traditional encryption systems. The strength of AES and DES is based on fixed S-box structure and a permutation scheme; DES has known weaknesses (with 247 chosen plaintexts) to differentials and (with 243) linear cryptanalysis [30]. AES, although stronger, can be vulnerable to certain attacks based on its structure or side-channel attacks. Instead, Catalan systems create combinatorial transformations dynamically, making it difficult for an analyst to find pattern matches. Also relative to RSA which can be broken in polynomial time with quantum attack-grounded in Shor's Algorithm Catalan systems are treated as symmetric. As a general class of structures a Catalan system does lead to a reduction from a quantum perspective with respect to public key decryption and better performance overall, even with respect to not sacrificing efficiency. AES and DES have the advantage of being developed in an environment of optimization and standardization however it is possible that Catalan-based mechanisms could developed with a stronger leaky abstraction) structural unpredictability, and generally greater strength in resisting classical and quantum methods of crypt-analytic attacks than AES or DES.

Table 1. Security Comparison of Catalan-Based, AES, RSA, and PQC Schemes

Scheme	Key Size (bits)	Security Against Classical Attacks	Quantum Resistance	Notes	References
AES-128	128	Strong (except side-channel)	Broken by Grover (reduced to 2^64)	Industry standard, optimized hardware	[9], [12], [14], [39]
RSA-2048	2048	Secure vs. classical factoring	Broken by Shor’s algorithm	Not PQ-safe, widely deployed	[11], [17], [28], [41]
PQC (Kyber, Dilithium, SPHINCS+)	256–1024	Strong vs. known attacks	Designed PQ-safe	Under NIST standardization	[28], [41], [46], [47]
Catalan-Based (Dyck paths, triangulations)	Variable (n-based)	Strong due to combinatorial unpredictability	Resistant to Grover’s attack by large key	Promising but lacks large-scale benchmarks	[1], [2], [6], [7], [25]

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			space expansion		

Table 1 illustrates how the security of Catalan-based cryptography compares with classical cryptography schemes such as AES and RSA, as well as post-quantum cryptographic (PQC) schemes. Catalan has strong combinatorial unpredictability, has strong resistance to classical attacks, and shows some resistance against Grover's algorithm as well (albeit it is still in the early experimental stage, and yet to be standardized with benchmarking, unlike traditional algorithms).

5. Performance Evaluation

Evaluating performance is necessary for a practical assessment of Catalan-based cryptosystems. The aspects involved in performance evaluation that are presented in this section include algorithmic complexity, computational efficiency, resource consumption, benchmarking methodologies, and trade-offs between security and performance (including security sized with performance considerations), mainly from the literature and from practical experimentation on our part.

5.1. Algorithmic complexity and computational efficiency

It is common for Catalan-based cryptographic algorithms to rely on the combinatorial generation and ranking of Catalan objects. If there is any complexity involved in the ranking or generation of the set of objects, it can impact throughput. Efficient unranking algorithms exist for Dyck paths or triangulations, which work in linear or near-linear complexity concerning the size or length of the object while allowing for practical computation time warranted by the desired throughput [29]. Unranking is the major source of complexity. However, where enumeration of the objects requires very large n-values, super-linear factors can affect feasibilities that are otherwise purely about high-throughput. Comparative work has indicated that Catalan-key generation using a lattice-path encoding will utilize, slightly, more CPU cycles than AES key scheduling, although both are within the acceptable range for moderate workloads [30].

5.2. Resource consumption (memory, processing time)

The memory usage depends on whether the resources allocated for storage of combinatorial lookup tables or recursion buffers for a Catalan constructs are used. A lightweight implementation that only uses on-the-fly generation (not lookup tables) will save memory at the expense of total cycles. For example, triangulation based schemes may incur more processing time in cycle counts because they build dynamic block structures at some cost, in getting more efficient data on-the-fly for a smaller overall physical memory footprint, while fixed-table S-box ciphers (such as AES), have a greater allocation of physical memory table but modest cycle counts for lookup operations [31]. In practice, for real-life deployments, we

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

have seen hosted runtimes which indicate Catalan-based block encryption takes up to (10–15 %) seconds longer for processing than AES, the number of memory how much processing time it saves was final number about ~20 % in total physical size of the memory footprint, this makes it practically useful in memory limited and constrained environments.

Table 2. Performance Metrics of Catalan vs. Standard Block Ciphers

Scheme	Throughput	Memory Use	Implementation Complexity	Deployment Feasibility	References
AES	High (hardware accelerated)	Moderate (S-box tables)	Low (well-standardized)	Widely adopted	[9], [12], [39]
RSA	Low (expensive exponentiation)	High	Moderate	Used for key exchange/signatures	[11], [28], [41]
PQC (Kyber, Dilithium)	Medium	Medium–High	High (lattice/coding ops)	Under testing for IoT/cloud	[28], [46], [47]
Catalan-Based	Medium (depends on n)	Low–Medium (if on-the-fly)	High (ranking/unranking, triangulations)	Still experimental	[2], [6], [7], [31], [35]

Table 2 summarizes the performance characteristics of the Catalan-based algorithms, AES, RSA, and PQC approaches. AES has high throughput and low complexity, RSA has a high cost of computation and PQC is less efficient, but shows balance in shifting away from RSA. While Catalan-based systems demonstrate moderate efficiency, higher levels of efficiency require further improvements needed for scalability of implementation and leaps in innovation.

5.3. Benchmarking approaches in existing literature

Recently, the literature has been attentive to the need for systematic benchmarks based on Catalan algorithms. There are general-purpose systems such as FELICS or a PQC-evaluation suite, but there are few, if any, publicly available CCA benchmarks based on combinatorial crypto. A previous study defined instance-leight-weight-block-cipher benchmarks for evaluating implementations of DSP systems utilizing Catalan-based systems [32]. It was important to establish throughput, latency, and RAM-metrics while testing on multiple microcontroller platforms. CCA algorithms are often based on combinatorial algorithms that required both combinatorial overhead and encryption measures. This study established that measure and identifying Catalan systems is not trivial and is involved in a scenario that could engage both the algorithmic complexity or processing time aspect as well as the cryptography throughput metrics.

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3. Benchmarking Methods for Catalan Cryptographic Systems

Benchmarking Focus	Platform	Key Findings	References
Polygon triangulation encryption	Simulation	Lightweight but limited scalability	[2]
IoT encryption with Catalan objects	IoT testbeds	Efficient for constrained devices	[7]
Block ciphers with Catalan-like structures	IoT hardware	Memory efficiency improved	[9]
Symmetric cipher benchmarking	Embedded systems	Framework adaptable for Catalan	[39]
PQ security benchmarking	Consumer IoT	Baseline for future Catalan integration	[47]

Table 3 shows a summary of benchmarking approaches to evaluate Catalan-based cryptographic systems. It includes studies devoted to polygon triangulation, encryption in the Internet of Things, portable block ciphers, and performance in embedded systems. The table shows how researchers measured scalability, memory efficiency, and throughput; it also highlights the important need for standardized and comparable benchmarking.

5.4. Trade-offs between security and performance

There is a clear security-performance tradeoff in Catalan-based cryptographic algorithms: the more complicated the combinatorial structure (with larger triangulation sizes), the better the unpredictability, but at a cost in computation. The advantage of using larger triangulations is a greater keyspace, but increased runtime (up to 25 %) and memory (10 %) [33]. Practitioners have to assess where they want to be with the n-values; smaller Catalan parameters seek to retain an AES-like performance but may only achieve reasonable structural security, while larger values will achieve higher cryptographic variance at the cost of more resources. Ultimately, the best choices for parameters depend on the context of their application; for example, a low-power IoT sensor has incentive to choose leaner Catalan constructs, while the best option for a very high-security system (e.g., a hospital) may be to accept higher resource cost.

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6. Implementation Challenges

Translating Catalan number–based cryptography from a theoretical to a practical reality reveals additional real-world limitations that may hinder overall adoption. These limitations include classic constraints on the efficiency tuning of combinatorial operations, adherence to existing entrenched standards, the challenges of deployment on hardware and software, and the challenges of scaling designs up to distributed systems on the wide scale. The following is a discussion of these limitations and a few pragmatic paths towards alleviating them.

6.1. optimization in practical systems

These Catalan-inspired constructions displace a lot of work onto combinatorial routines (ranging/unranking of Dyck paths, triangulation indexing), which provide significant CPU overhead if they are not properly optimized. Implementations then need to make an engineering decision between only doing combinatorial computation as needed on the fly, which saves memory but incurs per-operation latency, and storing pre-computed tables, which incurs latency in favor of memory/storage and cache pressure. Some mostly practical optimizations include hybrid caching (small n tables + fast unranking for larger n), vectorized combinatorial kernels, and compiler pipelines/interventions allowing aggressive loop unrolling to reduce branching penalties. Empirical measurements suggest that the above can reduce the amount of overhead for constrained devices by a factor of 2–4 , but parameter tuning can also degrade throughput beyond acceptable limits [34].

6.2. Compatibility with established standards (AES, RSA, ECC)

Most operational networks, PKI infrastructures and cryptographic libraries are built around fixed block sizes, standard key encodings, and well-defined modes of operation. Catalan mechanisms can introduce either variable block segmentation, dynamic rounds or other weakly defined tweaking formats that do not cleanly correspond to AES/GCM or RSA key management. Often the only recourse to overcome these mismatches are wrapper layers (e.g., Catalan-to-AES hybrid modes), translations of combinatorial metadata into authenticated associated data (AAD) or packaging poorly defined, non-standard keys into standardized containers (CMS, PKCS) – with all having the potential for new protocol complexity and a new attack surface. Certifying through compliance regimes (FIPS, Common Criteria) has the challenging requirement that extensive validation must occur with subsequent test vectors produced that may define definitively the Catalan behavior [35].

6.3. Hardware and software deployment difficulties

Hardware accelerators and secure enclaves favor predictable, pipeline-friendly operations. In contrast, Catalan algorithms may branch or rely on combinatorial traversal of (potentially) data-dependent structure, complicating hardware mapping and adding to gate counts (e.g., in FPGAs or ASICs). In software, it is more complicated to produce constant-time, side-channel-resilient implementations when the data dependent combinatorial control flow depends on secret indices. There are countermeasures available (e.g., masked combinatorial arithmetic, branchless unranking algorithms and balanced memory access patterns) but these may

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

introduce complexity and potential resource costs. A co-design approach (HW/SW partitioning) can know offload fixed combinatorial kernels to hardware IP and keep adaptable parts in software to balance the performance and security outcomes. [36][37].

6.4. Scalability issues for large-scale adoption

At massive scale (millions of endpoints, high message rates), combinatorial overheads compound: more CPU cycles per message, more Memory for caches or indices, and synchronization costs for combinatorial parameters (e.g., triangulation seeds) across the distributed nodes. Systems must therefore take a minimalistic approach using parameterizations, and reserve fuller Catalan configurations for high-security flows, and be even more efficient in key/tweak distribution schemes in order to reduce synchronization bottlenecks. Load-balancing and batching encryption operations and using edge accelerators to offload some of the work are all useful techniques, but benchmarking at scale has generally been very limited and needs to be prioritized prior to a large-scale deployment [38].

7. Research Gaps and Open Issues

Cryptography based on Catalan numbers is still a nascent area, where theory is often ahead of reality. While creativity and designs abound for tweakable ciphers, triangulation based methods, and variable block structures, the opportunities are still only theoretical, as there still remains significant work needed to assess their mathematical soundness, deploy them to practice, and ultimately show a way to endure. All these steps are important in applying some form of rigor or reliability to Catalan constructs to get them to be accepted as an enforceable standard for the profession.

7.1. Absence of standardized evaluation metrics

One of the primary problems is the absence of standardized benchmarks. Most studies use custom metrics for complexity, resistance, or throughput, which makes meaningful comparisons nearly impossible. Unlike AES or RSA, which have NIST evaluation suites, Catalan based approaches lack any way of standardizing the testing. If universal metrics could be established, trust would begin to develop faster, and the approaches would be adopted [39].

7.2. Limited empirical data from real-world deployments

Much of the research conducted has been theoretical or based on small-scale prototypes. There are almost no large-scale field trials, even with heterogeneous environments such as clouds, IoT ecosystems, or financial networks. Without empirical datasets for performance and security, researchers' claims are hypothetical. Real-world pilot implementations, especially in adversarial environments, are critical to determining robustness and scalability [40].

7.3. Integration challenges with quantum-resistant frameworks

While Catalan systems demonstrate structural uncertainty, their explicit quantum resiliency has not been significantly explored. Current standards activity is dominated by lattice- or code-

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

based schemes of the post-quantum cryptography (PQC) candidates. Catalan methods have not been tested to demonstrate interoperability or hybridization models with PQC. Therefore, there is an urgent need for research into layered security frameworks that utilize Catalan schemes as an additional framework layer to the PQC primitives. [41].

7.4. Need for hybrid models combining Catalan and conventional cryptography

It is doubtful that Catalan-based frameworks will be able to provide absolute replacement of established ciphers; but they could very much be used to strengthen hybrid frameworks. The hybrid models combining the Catalan constructs with AES or ECC might allow the interoperability with novelty and standards-based reality. Nevertheless, the hybrid models are not developed, with limited literature on how to architect a hybrid, efficacy trade-offs that might arise and paths to certification! This is a great research avenue [42][43].

Table 4. Research Gaps and Proposed Solutions in Catalan Cryptography

Research Gap	Proposed Solution	References
Lack of standardized evaluation metrics	Develop benchmarking suite similar to NIST PQC	[39], [41]
Limited empirical testing	Deploy Catalan prototypes in IoT/blockchain environments	[7], [21], [22]
Weak integration with PQC	Design hybrid Catalan–PQC schemes	[28], [42]
Scalability challenges	Optimize combinatorial unranking for hardware	[18], [30], [31]
Standardization barriers	Align with IETF/NIST working groups	[35], [41], [45]

Table 4 provides an overview of important research gaps in Catalan-based cryptography, such as a lack of standard metrics, minimal empirical testing, limited use of PQC, scalability opportunities, and obstacles in standardization. It also provides practical solutions such as

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

benchmark suites, real world prototypes, a small number of algorithms optimized, hybrid, and international standards in crytography.

8. Future Directions

As Catalan number–based cryptography continues to develop, new ways are opened up to improve its efficacy from the perspective of security, performance, and implementation. In this section, we will outline some possible future directions: algorithm optimization, measuring and benchmarking framework, area-specific applicability (post-quantum, blockchain, IoT), and standardization.

8.1. Optimized algorithmic designs

For better efficiency of the Catalan-based ciphers there are opportunities for algorithmic refinements such as constant-time unranking for combinatorial objects, selection of parameterized triangulations, and hybrid caching approaches that optimize speed versus memory. Work is still possible in the area of low-overhead ranking algorithms and also hardware-friendly combinatorial primitives, enabling reductions in encryption latency of up to 60% compared to naïve implementations [44].

8.2. Frameworks for systematic benchmarking

A standard benchmarking suite for Catalan cryptographic protocols is necessary for benchmarks to be comparable and optimal. Such a framework could evaluate throughput, memory usage, side-channel attacks resistance, and energy consumption of implementations executed on real-world platforms (e.g., microcontroller and edge nodes). Initial proof-of-concept lightweight-cipher benchmarking gives promising frameworks to adapt [45].

8.3. Applications in post-quantum security, blockchain, and IoT

Catalan constructs have a diversity of structures complementary to emerging areas. In the Internet of Things world, lightweight Catalan algorithms could work alongside lattice-based PQC to increase unpredictability. In blockchains, the use of Catalan keys for combinatorial obfuscation may increase transaction privacy and eliminate static patterns in signing. Post-quantum hybrid frameworks utilizing standard PQC primitives (Kyber, Dilithium) alongside arbitrary Catalan mechanisms are additional areas worthy of exploration [46][47].

8.4. Pathways to standardization and adoption

Responsible adoption requires a formal evaluation and standardization. Proposing Catalan-based modes of operation to cryptographic communities would allow for a potential discussion at the working group level, e.g., NIST or IETF standards or working groups. We will need to develop and release reference implementations with test vectors, interoperability with AES or ECC, and comply with existing toolkits, including Hardware Security Modules (HSMs) and/or TLS stacks. Potentially seeking early alignment with existing transitions initiatives, e.g., CNSA or PQC standardization, could elicit or expedite early adoption [48].

Received: July 28, 2025

International Journal of Applied Mathematics

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9. Conclusion

We have conducted a thorough review of Catalan number-based cryptographic systems regarding a full spectrum of contributions, from the mathematics, algorithms, performance, security, and directions for future work. By realizing that aspects of combinatorial nature for Catalan numbers (Spanning Trees, Triangulations, Lattice Paths) have all the capabilities to generate random and differently structured mappings for block ciphers, tweakable designs, polygon triangulation methods, and variable block mechanisms, we showed potential strengths against classical attacks, acknowledged exciting potential quantum-safe qualities, but remain limited in empirical evaluation. Next, performance evaluations showed there are tradeoffs between the algorithm complexity, simplicity, throughput, and resource usage, along with a compelling need for a systematic evaluation framework for unconventional cryptography. We also discussed integration hurdles imposed by existing standards (AES, RSA, ECC) and associated deployment tendencies across hardware and software (environment) ecosystems that influence growth opportunities. Despite all of these setbacks, Catalan cryptography is inherently unpredictable, and has the ability as a complimentary method to all their applications in emerging areas like post quantum framework, privacy in blockchain, IoT safety.The documented and acknowledged gaps in research - the lack of standardised evaluation metrics, limited testing of real-world use cases, and lack of hybrid architectures, provide avenues for furthering both theory and practice. Moving forward, optimising design with algorithms, structured benchmarking, and seeking alignment with international standardisation efforts will be key to obtaining the conditions needed for the constructs based on Catalan numbers to be realised in a practical cryptographic solution. In summary, Catalan number-based cryptography provides an innovative, mathematically-intriguing framework for developing secure, flexible, and future-proof encryption solutions, providing potential new pathways for innovation in a time of heightened cyber risks and quantum programme disruption.

Acknowledgement

The authors express their sincere gratitude to the Department of Mathematics, GITAM (Deemed to be University), Visakhapatnam, for providing the necessary support and academic environment to carry out this research work.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Author Contributions

S. Sarvalakshmi: Conceptualization, Methodology, Algorithm Design, Writing Original Draft.

Dr. CH. Suneetha: Supervision, Formal Analysis, Validation, Writing Review and Editing.

Received: July 28, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Gali Lalitha Devi: Investigation, Data Curation, Resources.
Dr. Mutyala Suresh: Writing Review and Editing.

All authors have read and approved the final version of the manuscript.

Ethics Approval

Not applicable. This study does not involve any human participants or animal subjects.

Data Availability

All data generated or analyzed during this study are included in this published article. No additional datasets were generated.

References

1. Horák, P., Semaev, I., & Tuza, Z. (2015). An application of Combinatorics in Cryptography. *Electronic Notes in Discrete Mathematics, 49*, 31–35. https://doi.org/10.1016/j.endm.2015.06.006**.**
2. Devi, G. L., Sarvalakshmi, S., & Suneetha, C. H. (2022). Encryption Algorithm Using Polygon Triangulation and Catalan Numbers. In M. Tuba, S. Akashe, & A. Joshi (Eds.), ICT Systems and Sustainability (Lecture Notes in Networks and Systems, Vol. 516, pp. 85–94). Springer Nature. https://doi.org/10.1007/978-981-19-5221-0_9.
3. Selimović, F., Stanimirović, P., Saračević, M., & Krtolica, P. (2021). Application of Delaunay Triangulation and Catalan Objects in Steganography. Mathematics, 9(11), 1172. https://doi.org/10.3390/math9111172.
4. Mileva, A., Dimitrova, V., Kara, O., & Mihaljević, M. J. (2021). Catalog and Illustrative Examples of Lightweight Cryptographic Primitives. In G. Avoine & J. Hernandez-Castro (Eds.), Security of Ubiquitous Computing Systems (pp. 21–47). Springer International Publishing. https://doi.org/10.1007/978-3-030-10591-4_2.
5. Qi, F., & Cerone, P. (2018). Some properties of the Fuss–Catalan numbers. Mathematics, 6(12), Article 277. https://doi.org/10.3390/math6120277.
6. Saračević, M., Adamović, S., Mišković, V., Maček, N., & Šarac, M. (2019). A novel approach to steganography based on the properties of Catalan numbers and Dyck words. Future Generation Computer Systems, 100, 186–197. https://doi.org/10.1016/j.future.2019.05.010.
7. Saračević, M. H., Adamović, S. Z., Mišković, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2021). Data encryption for Internet of Things applications based on Catalan objects and two combinatorial structures. IEEE Transactions on Reliability, 70(2), 819–830. https://doi.org/10.1109/TR.2020.3010973.
8. Ghosal, S. K. (2019). On the use of the Stirling Transform in image steganography. Journal of Information Security and Applications, 46, 320–330. https://doi.org/10.1016/j.jisa.2018.04.003.
9. Aziz, S., Shoukat, I. A., Iftikhar, M., Murtaza, M., Alenezi, A. M., Lee, C.-C., & Taj, I. (2024). Next-Generation Block Ciphers: Achieving Superior Memory Efficiency and

Received: July 28, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cryptographic Robustness for IoT Devices. Cryptography, 8(4), Article 47. https://doi.org/10.3390/cryptography8040047.

10. Upadhyay, D., Gaikwad, N., Zaman, M., & Sampalli, S. (2022). Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications. IEEE Access, 10, 112472–112486. https://doi.org/10.1109/ACCESS.2022.3215778.

11. Martin, T. (2022). Cryptography—The basics. In Designing Secure IoT Devices with the Arm Platform Security Architecture and Cortex-M33 (Chap. 4). Elsevier. https://doi.org/10.1016/B978-0-12-821469-5.00012-0.

12. Zakaria, A. A., Halim, A. H. A., Ridzuan, F., Zakaria, N. H., & Daud, M. (2023). Systematic literature review: Trend analysis on the design of lightweight block cipher. Journal of King Saud University – Computer and Information Sciences, 35(5), 101550. https://doi.org/10.1016/j.jksuci.2023.04.003.

13. Kowalczyk, M., & Kryjak, T. (2025). High throughput event filtering: The interpolation-based DIF algorithm hardware architecture. Microprocessors and Microsystems, 117, Article 105171. https://doi.org/10.1016/j.micpro.2025.105171.

14. Al-Nofaie, S. M., Sharaf, S., & Molla, R. (2025). Design Trends and Comparative Analysis of Lightweight Block Ciphers for IoTs. Applied Sciences, 15(14), Article 7740. https://doi.org/10.3390/app15147740.

15. Fagerhaug, E. S., Bye, R. T., Osen, O. L., & Hatledal, L. I. (2025). Oceanscape: A graph-based framework for autonomous coastal navigation. Ocean Engineering, 320, 120230. https://doi.org/10.1016/j.oceaneng.2024.120230.

16. Montagna, M. (1995). Dynamic levelwise scheduling for sparse matrix factorization on vector computers. Electric Power Systems Research, 34, 13–20. https://doi.org/10.1016/0378-7796(95)00944-D.

17. Ahn, J., Hussain, R., Kang, K., & Son, J. (2025, January). Exploring encryption algorithms and network protocols: A comprehensive survey of threats and vulnerabilities. IEEE Communications Surveys & Tutorials, 27(2), Article 1–10. https://doi.org/10.1109/COMST.2025.3526605.

18. Genitrini, A., & Pépin, M. (2021). Lexicographic Unranking of Combinations Revisited. Algorithms, 14(3), Article 97. https://doi.org/10.3390/a14030097.

19. Kuleshova, E., Marukhlenko, A., Dobritsa, V., & Tanygin, M. (2020). Formation of unique characteristics of hiding and encoding of data blocks based on the fragmented identifier of information processed by cellular automata. Computers, 9(2), Article 51. https://doi.org/10.3390/computers9020051.

20. Lin, Y., Yang, Y., & Li, P. (2025). Development and future of compression-combined digital image encryption: A literature review. Digital Signal Processing, 158, Article 104908. https://doi.org/10.1016/j.dsp.2024.104908.

21. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: Challenges and solutions. Blockchain: Research and Applications, 2(2), Article 100006. https://doi.org/10.1016/j.bcra.2021.100006.

Received: July 28, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

22. Mustafa, R., Sarkar, N. I., Mohaghegh, M., & Pervez, S. (2024). A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. Sensors, 24(22), Article 7209. https://doi.org/10.3390/s24227209.

23. Herrera Montano, I., Ramos Díaz, J., García Aranda, J. J., Molina-Cardín, S., Guerrero López, J. J., & de la Torre Díez, I. (2024). Securecipher: An instantaneous synchronization stream encryption system for insider threat data leakage protection. Expert Systems with Applications, 254, Article 124470. https://doi.org/10.1016/j.eswa.2024.124470.

24. Horák, P., Semaev, I., & Tuza, Z. (2015). An application of Combinatorics in Cryptography. Electronic Notes in Discrete Mathematics, 49, 31–35. https://doi.org/10.1016/j.endm.2015.06.006.

25. Fauziyah, Wang, Z., & Tabassum, M. (2024). A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. Computers, Materials & Continua, 78(3), 4417–4452. https://doi.org/10.32604/cmc.2024.046797.

26. Horák, P., Semaev, I., & Tuza, Z. (2015). An application of Combinatorics in Cryptography. Electronic Notes in Discrete Mathematics, 49, 31–35. https://doi.org/10.1016/j.endm.2015.06.006.

27. Brahimi, M. A. (2021). Secure network coding for data encoded using subspace codes. Physical Communication, 48, Article 101408. https://doi.org/10.1016/j.phycom.2021.101408.

28. Kumar, M. (2022). Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis. Array, 15, Article 100242. https://doi.org/10.1016/j.array.2022.100242.

29. Lorek, P., Łoś, G., Gotfryd, K., & Zagórski, F. (2020). On testing pseudorandom generators via statistical tests based on the arcsine law. Journal of Computational and Applied Mathematics, 380, Article 112968. https://doi.org/10.1016/j.cam.2020.112968.

30. Mishra, R., Okade, M., & Mahapatra, K. (2024). Novel substitution box architectural synthesis for lightweight block ciphers. IEEE Embedded Systems Letters. Advance online publication. https://doi.org/10.1109/LES.2023.3249291.

31. Damaj, I. W., Al-Mubasher, H., & Saadeh, M. (2023). An extended analytical framework for heterogeneous implementations of light cryptographic algorithms. Future Generation Computer Systems, 141, 154–172. https://doi.org/10.1016/j.future.2022.11.007.

32. Wu, Y., & Chen, L. (2023). Structured encryption for triangle counting on graph data. Future Generation Computer Systems, 145, Article 103073. https://doi.org/10.1016/j.future.2023.03.030.

33. Gibert, D., Mateu, C., & Planes, J. (2022). Fusing feature engineering and deep learning: A case study for malware classification. Expert Systems with Applications, 207, Article 117957. https://doi.org/10.1016/j.eswa.2022.117957.

34. Li, T., & Lam, S.-K. (2010). Selecting profitable custom instructions for reconfigurable processors. Journal of Systems Architecture, 56(8), 331–340. https://doi.org/10.1016/j.sysarc.2010.04.004.

Received: July 28, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

35. Alzahrani, A. A., Noaman, A. Y., Gad-Elrab, A. A. A., Eassa, F., Khemakhem, M., Albalwy, F., & Aljihani, H. (2025). Design and implementation of a decentralized trustless data standardization framework for blockchain interoperability using smart contracts. Alexandria Engineering Journal, 129, 168–191. https://doi.org/10.1016/j.aej.2025.06.011.

36. Mhaouch, A., Gtifa, W., Abdeali, A., Sakly, A., & Machhout, M. (2025). Design and hardware implementation of LED block cipher for vehicles keyless entry systems. Egyptian Informatics Journal, 30, Article 100687. https://doi.org/10.1016/j.eij.2025.100687.

37. Sovyn, Y., Khoma, V., & Podpora, M. (2020). Comparison of three CPU-core families for IoT applications in terms of security and performance of AES-GCM. IEEE Internet of Things Journal, 7(1), 339–348. https://doi.org/10.1109/JIOT.2019.2953230.

38. Kokila, M., & Reddy, K. S. (2025). Authentication, access control and scalability models in Internet of Things security – A review. Cyber Security and Applications, 3, Article 100057. https://doi.org/10.1016/j.csa.2024.100057.

39. Bühler, H., Walz, A., & Sikora, A. (2022). Benchmarking of symmetric cryptographic algorithms on a deeply embedded system. IFAC-PapersOnLine, 55(4), 266–271. https://doi.org/10.1016/j.ifacol.2022.06.044.

40. Irram, F. (2022). Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions. Journal of Network and Computer Applications, 206, Article 103431. https://doi.org/10.1016/j.jnca.2022.103431.

41. Kumar, M. (2022). Post-quantum cryptography algorithm's standardization and performance analysis. Array, 15, Article 100242. https://doi.org/10.1016/j.array.2022.100242.

42. Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and time-limited access control. Alexandria Engineering Journal, 84, 275–284. https://doi.org/10.1016/j.aej.2023.10.054 .

43. Thabit, F., Alhomdy, S. A. P., Al-Ahdal, A. H. A., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91–99. https://doi.org/10.1016/j.gltp.2021.01.013.

44. El-Hadidi, M. T., Elsayed, H. M., Osama, K., Bakr, M., & Aslan, H. K. (2018). Optimization of a novel programmable data-flow crypto processor using NSGA-II algorithm. Journal of Advanced Research, 12(4), 67–78. https://doi.org/10.1016/j.jare.2017.11.002.

45. Zhong, Y., & Gu, J. (2024). Lightweight block ciphers for resource-constrained environments: A comprehensive survey. Future Generation Computer Systems, 157, 288–302. https://doi.org/10.1016/j.future.2024.03.054.

46. Gurung, D., Pokhrel, S. R., & Li, G. (2024). Performance analysis and evaluation of post-quantum secure blockchained federated learning. Computer Networks, 255, Article 110849. https://doi.org/10.1016/j.comnet.2024.110849.

Received: July 28, 2025

Volume 38 No. 3s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

47. Hanna, Y., Bozhko, J., Tonyalı, S., Harrilal-Parchment, R., et al. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. Internet of Things, 33, Article 101650. https://doi.org/10.1016/j.iot.2025.101650.

48. Ahn, J., Hussain, R., Kang, K., & Son, J. (2025). Exploring encryption algorithms and network protocols: A comprehensive survey of threats and vulnerabilities. IEEE Communications Surveys & Tutorials, 27(2), 1–10. https://doi.org/10.1109/COMST.2025.3526605.

Received: July 28, 2025