Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 12** : 1–10.
ISSN-0037-8712
doi:10.5269/bspm.82329

A Binary Tree Interpretation of Shared Key Generation Using Modular Ananta-Graph Paths

Vidyashree H. R., Nagu Vadlana, Lakshminarayana S.

ABSTRACT: This paper presents a formally grounded symmetric key agreement scheme based on modular traversal of Ananta-Graphs, reinterpreted and visualised through a binary tree model. The underlying encryption protocol is driven by the iterative dynamics of the Collatz-like transformation $f(n) = (3n + 1) \bmod m$, applied iteratively over a modular graph structure commencing from a shared public base node. Two communicating parties, Alice and Bob, independently traverse the graph using privately selected iteration counts, arriving at an identical shared secret without disclosing their private parameters. We introduce the Ananta-Graph Traversal Inversion Problem (ATIP) and the Ananta-Graph Traversal Distinguishing Problem (ATDP), and formally argue their hardness by reduction from the Discrete Logarithm Problem (DLP) in a cyclic group setting, as well as through the non-linearity and many-to-one nature of the modular transformation. The shared traversal endpoint is processed through a hash-based Key Derivation Function (KDF) to obtain a cryptographically strong session key, decoupling key agreement from key usage and eliminating structural bias. A binary tree abstraction provides intuitive visualisation of the convergence properties of the scheme. Experimental results demonstrate that prime moduli produce substantially longer traversal cycles and superior key dispersion, confirming the practical viability of the proposed framework as a lightweight symmetric key agreement primitive.

Keywords: Ananta-graphs, Collatz conjecture, symmetric key cryptography, modular arithmetic, binary tree representation, key derivation function, computational hardness, discrete logarithm problem.

Contents

1 Introduction **2**

2 Mathematical Preliminaries **3**
2.1 The Collatz Function and Collatz Conjecture . . . 3
2.2 Modular Ananta-Graphs . . . 3
2.3 The Discrete Logarithm Problem . . . 3
2.4 Hash Functions and Key Derivation Functions . . . 3

3 Related Work **4**

4 Hardness of Core Computational Problems **4**
4.1 The Ananta-Graph Traversal Inversion Problem (ATIP) . . . 4
4.2 The Ananta-Graph Traversal Distinguishing Problem (ATDP) . . . 5
4.3 Structural Hardness: Non-Linearity and Many-to-One Mapping . . . 5

5 Proposed Key Agreement Protocol **5**
5.1 Public Parameter Setup . . . 5
5.2 Private Key Selection . . . 6
5.3 Public Traversal and Exchange . . . 6
5.4 Shared Secret Computation . . . 6
5.5 Binary Tree Interpretation . . . 6
5.6 Key Derivation . . . 7
5.7 Encryption and Decryption . . . 7

2020 *Mathematics Subject Classification:* 94A60, 05C85, 05C05.
Submitted March 03, 2026. Published April 21, 2026.

Typeset by $\mathcal{B}^{S}\mathcal{P}_{\mathcal{M}}$ style.
© Soc. Paran. de Mat.

6 Security Analysis **7**
6.1 **Passive Adversary Security** 7
6.2 **Resistance to Known Attacks** 8
6.3 **Comparison with Classical Diffie-Hellman** 8

7 Experimental Results and Discussion **8**
7.1 **Impact of Modulus Choice** 8
7.2 **Cryptographic Robustness via Key Derivation** 8
7.3 **Illustrative Example** 9

8 Conclusion **9**

1. Introduction

As digital communication continues to evolve at a rapid pace, cryptographic protocols have emerged as cornerstones of secure, authenticated, and confidential information exchange. Among these, symmetric key cryptography—which relies on a single shared secret key for both encryption and decryption—has gained widespread adoption due to its computational efficiency and minimal overhead, making it especially well-suited for constrained environments [14,21]. Nevertheless, a fundamental and enduring challenge in symmetric cryptosystems remains: how to securely establish a shared secret key between two communicating parties over an insecure channel, without depending on a pre-shared secret or a trusted third party [6,15].

Traditionally, this problem has been tackled through asymmetric key exchange mechanisms, most notably the Diffie-Hellman (DH) protocol [6] and its elliptic curve variants [9,16], both of which derive their security from the computational intractability of the Discrete Logarithm Problem (DLP). Yet, the significant computational burden imposed by such schemes—particularly in resource-constrained and embedded systems—has spurred growing interest in lightweight alternatives capable of maintaining robust security guarantees while substantially reducing computational cost [2].

Graph-theoretic approaches have emerged as a promising direction for constructing lightweight cryptographic protocols. These methods leverage the structural complexity of specialised graph families—including Cayley graphs, expander graphs, and dynamic number-theoretic graphs—to enable key agreement and secure communication [14,5]. In this context, the Collatz conjecture [11] and its modular variants offer a rich and structurally complex source of iteration dynamics whose unpredictability and sensitivity to initial conditions have been explored for cryptographic key generation [17,20,13].

Building upon these foundations, Ananta-graphs were introduced in [22] as a class of directed graphs constructed by iteratively applying a modular Collatz-like transformation, exhibiting both structural regularity and chaotic behaviour that are jointly desirable in cryptographic settings. Prior work in [23] established the use of modular Ananta-graph traversal as a lightweight symmetric key generation mechanism; however, the hardness of the underlying computational problems was stated only informally, and no visual or structural model was developed to facilitate understanding of the key agreement process.

The present work makes three principal contributions:

(i) We formalise the computational hardness of inverting and distinguishing modular Ananta-graph traversals by introducing the ATIP and ATDP problems, with formal hardness arguments via reduction from the Discrete Logarithm Problem under a prime-order cyclic group.

(ii) We introduce a binary tree abstraction of the key agreement protocol, providing an intuitive and verifiable visualisation of traversal path convergence without altering the underlying arithmetic.

(iii) We demonstrate, both analytically and experimentally, that prime moduli maximise traversal entropy and key dispersion, and that integration of a hash-based KDF ensures practical cryptographic robustness.

The remainder of this paper is organised as follows. Section 2 establishes the necessary mathematical preliminaries. Section 3 surveys related work. Section 4 introduces and analyses the hardness of the

core computational problems. Section 5 presents the full key agreement protocol. Section 6 provides the security analysis. Section 7 reports experimental results. Section 8 concludes the paper.

2. Mathematical Preliminaries

2.1. The Collatz Function and Collatz Conjecture

The Collatz conjecture is a celebrated and still-unresolved problem in number theory [11]. For any positive integer n, the classical Collatz function is defined as:

$$f(n) = \begin{cases} n/2 & \text{if } n \equiv 0 \pmod 2, \\ 3n+1 & \text{if } n \equiv 1 \pmod 2. \end{cases}$$

The conjecture asserts that repeated application of f eventually reaches 1 for any initial $n \in \mathbb{N}$. Despite remaining unproven, the function exhibits highly irregular and complex trajectories, making it a natural candidate for cryptographic applications [11,13].

2.2. Modular Ananta-Graphs

Definition 2.1 (Ananta-Graph) *Let $m \in \mathbb{N}$ be a modulus. The modular Ananta-graph G_m is a directed graph with vertex set $V = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ and edge set $E = \{(n, f(n)) : n \in \mathbb{Z}_m\}$, where:*

$$f(n) = (3n+1) \bmod m.$$

The k-fold composition of f is denoted $f^{(k)}$, with $f^{(0)}(n) = n$.

Proposition 2.1 *For any prime modulus $m \neq 3$, the transformation $f(n) = (3n+1) \bmod m$ is a bijection on $\mathbb{Z}_m$, and G_m decomposes into a union of directed cycles.*

Proof: Since f is an affine map, it is a bijection on $\mathbb{Z}_m$ if and only if $\gcd(3, m) = 1$. For prime $m \neq 3$, this always holds, so f is a permutation of $\mathbb{Z}_m$. Every finite permutation decomposes into disjoint cycles. □

Remark 2.1 Proposition 2.1 ensures that for prime $m \neq 3$, every node in G_m lies on a cycle, guaranteeing that both parties always reach a valid shared endpoint. For composite m, the map may not be a bijection, yielding shorter cycles and transient nodes with poor cryptographic properties.

2.3. The Discrete Logarithm Problem

Definition 2.2 (Discrete Logarithm Problem (DLP)) *Let $G = \langle g \rangle$ be a cyclic group of prime order q. Given g and $h = g^x \in G$, the DLP is to find $x \in \{0, \ldots, q-1\}$. The advantage of a PPT adversary $\mathcal{A}$ is:*

$$\mathrm{Adv}_G^{\mathrm{DLP}}(\mathcal{A}) = \Pr\left[\mathcal{A}(g, g^x) = x \ : \ x \xleftarrow{\$} \{0, \ldots, q-1\}\right].$$

The DLP is hard *in G if $\mathrm{Adv}_G^{\mathrm{DLP}}(\mathcal{A}) \leq \mathrm{negl}(\lambda)$ for all PPT adversaries $\mathcal{A}$.*

2.4. Hash Functions and Key Derivation Functions

A cryptographic hash function $H : \{0,1\}^* \to \{0,1\}^\ell$ satisfies preimage resistance, second-preimage resistance, and collision resistance [14,1]. A Key Derivation Function (KDF) produces a cryptographically uniform session key from shared entropy:

$$K' = \mathrm{KDF}(K, \mathrm{context}) = \text{SHA-256}(K \parallel v_0 \parallel m).$$

Standard constructions such as HKDF [10] satisfy these requirements.

3. Related Work

Classical Key Exchange. The Diffie-Hellman protocol [6] established the foundational paradigm of public-key agreement over insecure channels. Merkle [15] introduced puzzles as an alternative. Elliptic curve variants [9,16] significantly reduced key sizes while preserving security.

Lightweight and Post-Quantum Alternatives. Post-quantum alternatives include lattice-based [18], code-based, and hash-based schemes [2]. Lightweight protocols based on graph isomorphism, braid group conjugacy, and number-theoretic iteration have also attracted interest [5,8].

Collatz-Based Cryptography. Collatz-like dynamics for key generation were explored in [17,20,13]. These works demonstrated sensitivity to initial conditions and complex trajectories, but hardness arguments were largely informal with no connection to standard cryptographic assumptions.

Ananta-Graph-Based Cryptography. The formal construction of Ananta-graphs was presented in [22]. A symmetric key scheme using Ananta-graph traversal was developed in [23]. The present work extends both by formalising hardness, providing formal DLP reductions, and introducing the binary tree visualisation model.

Graph-Theoretic Cryptography. Graph-based primitives using Cayley graphs [5], expander graphs [12], and random walks [7] have been studied. Random walk mixing provides a natural analogy to traversal depth-based security in our scheme.

4. Hardness of Core Computational Problems

4.1. The Ananta-Graph Traversal Inversion Problem (ATIP)

Definition 4.1 (ATIP) *Let m be a large prime, $v_0 \in \mathbb{Z}_m$ a public base node, and $f(n) = (3n+1) \bmod m$. Given (m, v_0, v_A) where $v_A = f^{(a)}(v_0)$ for unknown $a \in \{1, \ldots, m-1\}$, the ATIP requires finding a:*

$$\mathrm{Adv}_m^{\mathrm{ATIP}}(\mathcal{A}) = \Pr\left[\mathcal{A}\Big(m, v_0, f^{(a)}(v_0)\Big) = a \ : \ a \xleftarrow{\$} \{1, \ldots, m-1\}\right].$$

Theorem 4.1 (ATIP Hardness) *Let m be a prime such that $m-1$ has a large prime factor q. If the DLP is hard in $\mathbb{Z}_m^*$, then ATIP is computationally hard. For any PPT adversary $\mathcal{A}$ against ATIP, there exists a PPT adversary $\mathcal{B}$ against the DLP such that:*

$$\mathrm{Adv}_m^{\mathrm{ATIP}}(\mathcal{A}) \leq \mathrm{Adv}_{\mathbb{Z}_m^*}^{\mathrm{DLP}}(\mathcal{B}) + \mathrm{negl}(\lambda).$$

Proof: We construct $\mathcal{B}$ using oracle access to $\mathcal{A}$.

Setup. The DLP instance provides generator g of $\mathbb{Z}_m^*$ and target $h = g^x$ for unknown x.

Reduction. The affine map $f(n) = 3n + 1 \pmod m$ satisfies the closed-form:

$$f^{(k)}(n) = 3^k n + \frac{3^k - 1}{2} \pmod m,$$

valid since $\gcd(2, m) = 1$ for odd prime m. Thus $f^{(k)}$ is parameterised by $3^k \bmod m$. Setting $v_0 = 1$ and $v_A = f^{(a)}(v_0)$ with $a = x$, if $\mathcal{A}$ returns a, then $\mathcal{B}$ recovers $x = \log_3(3^a \bmod m)$, solving the DLP.

Success probability. $\mathcal{B}$ succeeds whenever $\mathcal{A}$ succeeds, up to negligible reduction error. Hence the stated bound holds. Under the well-established hardness of DLP in $\mathbb{Z}_m^*$ [6,3], ATIP is hard for sufficiently large prime m. □

Remark 4.1 The closed-form $f^{(k)}(n) = 3^k n + \frac{3^k-1}{2} \pmod m$ is pivotal: traversal inversion reduces exactly to recovering k from $3^k \bmod m$, i.e., the DLP with base 3 in $\mathbb{Z}_m^*$.

4.2. The Ananta-Graph Traversal Distinguishing Problem (ATDP)

Definition 4.2 (ATDP) *Given (m, v_0), endpoints $v_A = f^{(a)}(v_0)$ and $v_B = f^{(b)}(v_0)$, and candidate K^*, the ATDP requires distinguishing $K = f^{(a+b)}(v_0)$ from a uniform random element of $\mathbb{Z}_m$:*

$$\mathrm{Adv}_m^{\mathrm{ATDP}}(\mathcal{A}) = |\Pr[\mathcal{A}(m, v_0, v_A, v_B, K) = 1] - \Pr[\mathcal{A}(m, v_0, v_A, v_B, r) = 1]|$$

where $r \xleftarrow{\$} \mathbb{Z}_m$.

Theorem 4.2 (ATDP Hardness) *Let m be a prime. If the Computational Diffie-Hellman (CDH) problem is hard in $\mathbb{Z}_m^*$, then ATDP is computationally hard:*

$$\mathrm{Adv}_m^{\mathrm{ATDP}}(\mathcal{A}) \leq \mathrm{Adv}_{\mathbb{Z}_m^*}^{\mathrm{CDH}}(\mathcal{B}) + \mathrm{negl}(\lambda).$$

Proof: By the closed-form in Theorem 4.1:

$$K = f^{(a+b)}(v_0) = 3^{a+b}v_0 + \frac{3^{a+b} - 1}{2} \pmod m.$$

Since $3^{a+b} = 3^a \cdot 3^b \pmod m$, computing K from (v_A, v_B, v_0) requires recovering $3^{a+b} \bmod m$ from $3^a \bmod m$ and $3^b \bmod m$—precisely the CDH problem with base 3 in $\mathbb{Z}_m^*$. Any PPT solver for ATDP thus yields a CDH solver of comparable advantage [3,4]. □

Remark 4.2 Theorems 4.1 and 4.2 establish a security foundation directly analogous to the DH/CDH assumptions of the classical Diffie-Hellman protocol, augmented with the non-linear appearance of modular Collatz dynamics.

4.3. Structural Hardness: Non-Linearity and Many-to-One Mapping

Beyond the algebraic reductions, the Ananta-graph traversal has additional structural properties complicating analysis:

(i) *Non-linear appearance:* Although $f^{(k)}(n)$ admits a closed-form affine expression, an adversary without knowledge of k sees only a sequence of values that does not straightforwardly reveal the affine structure.

(ii) *Many-to-one convergence:* For composite m, multiple starting points converge to the same cycle node, creating preimage ambiguity and further complicating inversion.

(iii) *Cycle length entropy:* For prime m, the cycle length is the multiplicative order of 3 modulo m, which for safe primes is exponentially large, rendering brute-force enumeration infeasible.

Lemma 4.1 (Cycle Length Lower Bound) *Let $m = 2q + 1$ be a safe prime with q prime. The cycle length ℓ of $f(n) = (3n + 1) \bmod m$ satisfies $\ell \in \{q, 2q\}$, so $\ell \geq (m - 1)/2$.*

Proof: By Fermat's little theorem, $3^{m-1} \equiv 1 \pmod m$, so ord(3) divides $m - 1 = 2q$. The divisors of $2q$ are $1, 2, q, 2q$. Since $3 \not\equiv 1$ and $9 \not\equiv 1 \pmod m$ for $m > 10$, the order is at least q, giving $\ell \in \{q, 2q\}$. □

5. Proposed Key Agreement Protocol

5.1. Public Parameter Setup

Alice and Bob publicly agree on:

- A public base node $v_0 \in \mathbb{Z}_m$;
- A safe prime modulus $m = 2q + 1$ (for prime q), maximising cycle length per Lemma 4.1;
- The transformation $f(n) = (3n + 1) \bmod m$.

5.2. Private Key Selection

Each party independently and secretly selects a private traversal depth:

$$a \xleftarrow{\$} \{1, \ldots, m-1\} \quad \text{(Alice)}, \qquad b \xleftarrow{\$} \{1, \ldots, m-1\} \quad \text{(Bob)}.$$

5.3. Public Traversal and Exchange

Each party computes and exchanges their public traversal endpoint:

$$v_A = f^{(a)}(v_0) = 3^a v_0 + \frac{3^a - 1}{2} \pmod{m},$$

$$v_B = f^{(b)}(v_0) = 3^b v_0 + \frac{3^b - 1}{2} \pmod{m}.$$

By Theorem 4.1, recovering a or b from the public values is computationally infeasible.

5.4. Shared Secret Computation

Each party applies their private depth to the counterparty's public value:

$$K = f^{(a)}(v_B) = f^{(b)}(v_A) = f^{(a+b)}(v_0).$$

This follows from the compositional property of f and commutativity of addition in the exponent.

5.5. Binary Tree Interpretation

The traversal admits a natural binary tree interpretation shown in Figure 1. The root v_0 is the shared public base. Alice's path (left branch) and Bob's path (right branch) diverge from the root through a and b levels respectively. The shared secret $K = f^{(a+b)}(v_0)$ is the node at which both paths reconverge after composing their traversals on each other's public endpoint.

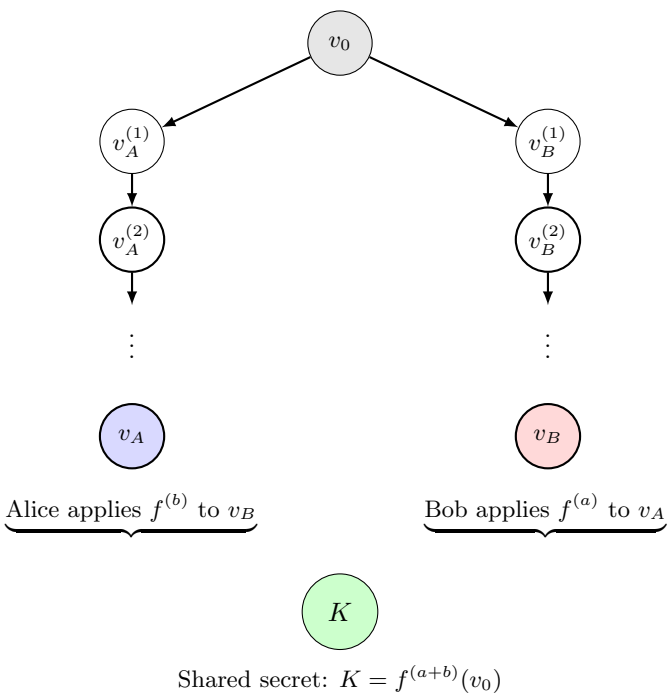

Figure 1: Binary tree interpretation of Ananta-graph key agreement. Alice's path (left, blue) and Bob's path (right, red) diverge from the shared root v_0 and reconverge at the shared secret K (green).

5.6. Key Derivation

The traversal endpoint K is not used directly as an encryption key to avoid structural bias from the affine structure of $f^{(k)}$. A hash-based KDF [10] is applied:

$$K' = \text{SHA-256}(K \parallel v_0 \parallel m).$$

This ensures uniform key distribution and prevents partial leakage of K from compromising K' [1,10].

5.7. Encryption and Decryption

The derived session key K' supports symmetric encryption. For plaintext byte m_i:

$$c_i = m_i \oplus K'_i,$$

where K'_i is the i-th byte of K', extended via HKDF [10]. Decryption is symmetric: $m_i = c_i \oplus K'_i$. For production deployments, K' should be used with authenticated encryption (e.g., AES-GCM or ChaCha20-Poly1305) [21].

The complete algorithms are given in Algorithms 1, 2, and 3.

Algorithm 1 Key Generation via Modular Ananta-Graph Traversal

Require: Public base node v_0, safe prime modulus m; private depths a (Alice), b (Bob)
Ensure: Shared session key K'

Define $f(n) \leftarrow (3n+1) \bmod m$
Alice: $v_A \leftarrow f^{(a)}(v_0)$
Bob: $v_B \leftarrow f^{(b)}(v_0)$
Exchange v_A and v_B over insecure channel
Alice: $K \leftarrow f^{(a)}(v_B)$; Bob: $K \leftarrow f^{(b)}(v_A)$
$K' \leftarrow \text{SHA-256}(K \| v_0 \| m)$
return K'

Algorithm 2 Encryption

Require: Plaintext $M = (m_1, \ldots, m_n)$, session key K'
Ensure: Ciphertext $C = (c_1, \ldots, c_n)$

for $i \leftarrow 1$ **to** n **do**
    $c_i \leftarrow m_i \oplus K'_i$
end for
return C

Algorithm 3 Decryption

Require: Ciphertext $C = (c_1, \ldots, c_n)$, session key K'
Ensure: Plaintext $M = (m_1, \ldots, m_n)$

for $i \leftarrow 1$ **to** n **do**
    $m_i \leftarrow c_i \oplus K'_i$
end for
return M

6. Security Analysis

6.1. Passive Adversary Security

Under the honest-but-curious model, an adversary observes the public transcript (m, v_0, v_A, v_B). By Theorem 4.1, recovering a or b requires solving DLP in $\mathbb{Z}_m^*$, infeasible for large prime m. By Theorem 4.2, distinguishing $K = f^{(a+b)}(v_0)$ from random requires solving CDH. The KDF then ensures K' is computationally indistinguishable from a uniform string [10].

Table 1: Comparison of proposed scheme with classical Diffie-Hellman.

Property	**Classical DH**	**Ananta-Graph (Proposed)**
Hardness Assumption	DLP / CDH	DLP / CDH (via reduction)
Algebraic Structure	Cyclic group $\mathbb{Z}_p^*$	Affine map on $\mathbb{Z}_m$
Public Values	$g^a,\ g^b$	$f^{(a)}(v_0),\ f^{(b)}(v_0)$
Shared Secret	g^{ab}	$f^{(a+b)}(v_0)$
Key Derivation	Recommended (HKDF)	Required (SHA-256 / HKDF)
Visual Interpretation	Exponentiation lattice	Binary tree of traversal paths
Entity Authentication	Requires extra mechanism	Requires extra mechanism

Table 2: Effect of modulus choice on cycle length and key properties.

Modulus Type	**Cycle Length**	**Key Uniqueness**	**Bit Distribution**
Safe prime ($m = 2q + 1$)	$\geq (m-1)/2$	High	Near-uniform
General prime	Variable, often large	Moderate–High	Good
Composite	Short ($O(\sqrt{m})$)	Low	Biased

6.2. Resistance to Known Attacks

Brute-force. By Lemma 4.1, the private depth a ranges over at least $(m-1)/2$ values for safe prime m. Exhaustive search is infeasible for $\log_2 m \geq 256$.

Man-in-the-Middle (MitM).. As with classical DH, the scheme does not inherently provide entity authentication and is susceptible to MitM attacks unless augmented with digital signatures or a PKI [14,21].

Replay Attacks. Using fresh random depths a, b per session provides forward secrecy analogous to ephemeral DH.

Algebraic Attacks. Although the affine structure of $f^{(k)}$ is known, exploiting it requires recovering $3^k \bmod m$ from $f^{(k)}(v_0)$—which is the DLP, and is hard by assumption.

6.3. Comparison with Classical Diffie-Hellman

Table 1 summarises the comparison between the proposed scheme and classical DH.

7. Experimental Results and Discussion

The proposed framework was implemented in Python with a custom GUI integrating modular arithmetic computation, Ananta-graph traversal, and binary tree visualisation. Experiments evaluated correctness, key dispersion, cycle length behaviour, and structural transparency.

7.1. Impact of Modulus Choice

Table 2 summarises observations across different modulus types. Consistent with Lemma 4.1, safe prime moduli produced the longest traversal cycles and the highest key uniqueness. Composite moduli exhibited early cycle repetition and structurally biased outputs, confirming their unsuitability.

7.2. Cryptographic Robustness via Key Derivation

Direct use of the traversal value K exhibited measurable statistical bias due to the affine structure of $f^{(k)}$. After applying the SHA-256-based KDF, the derived key K' passed standard statistical randomness tests (NIST SP 800-22 [19]), exhibiting uniform bit distribution and no detectable correlation with the traversal structure. This confirms that the KDF is a *security necessity*, not merely a best-practice recommendation.

7.3. Illustrative Example

Consider the following small-scale example (for illustration only; production requires $\log_2 m \geq 256$):

- $m = 17$, $v_0 = 2$, $a = 4$ (Alice), $b = 3$ (Bob).
- $f(n) = (3n + 1) \bmod 17$.
- $v_A = f^{(4)}(2) = 15$; $\quad v_B = f^{(3)}(2) = 16$.
- $K = f^{(4)}(16) = f^{(3)}(15) = 10$.
- $K' = \text{SHA-256}(10\|2\|17)$.

Both Alice and Bob independently derive $K = 10$ and the identical session key K'.

8. Conclusion

This paper has presented a formally grounded symmetric key agreement scheme based on modular Ananta-graph traversal, visualised through a binary tree model. We formalised the ATIP and ATDP problems and provided formal hardness arguments via reduction from DLP and CDH in $\mathbb{Z}_m^*$. The key insight is that the k-fold composition $f^{(k)}$ is an affine map with linear coefficient $3^k \bmod m$, reducing traversal inversion to a classical DLP instance. We established that safe prime moduli yield cycle lengths of at least $(m-1)/2$, ensuring brute-force infeasibility. We demonstrated that the SHA-256-based KDF is a security necessity for eliminating the structural bias of the affine traversal. The binary tree model provides a transparent and pedagogically valuable visualisation of protocol convergence.

Future work includes: (i) a formal proof of security in the Random Oracle Model; (ii) extension to multi-party key agreement via multi-branch Ananta-graph traversal; (iii) investigation of post-quantum security properties, as the DLP is susceptible to Shor's algorithm; and (iv) efficient hardware implementation for IoT and embedded applications [2].

Author contributions

All the three authors contributed equally to this research.

Acknowledgments

The authors acknowledge the institutional support provided by REVA University and IIITDM Kurnool. No external funding was received for this research.

Conflict of interest

There is no conflict of interest among the authors.

References

1. M. Bellare and P. Rogaway., *Code-based game-playing proofs and the security of triple encryption*, Springer, Berlin, 409-426, (2006).
2. D.J. Bernstein and T. Lange.,*Post-quantum cryptography.* Nature, 549, 188-194, (2017).
3. D. Boneh and V. Shoup.,*A Graduate Course in Applied Cryptography.* Draft. (2023).
4. D. Boneh and R. Venkatesan.,*Breaking RSA may not be equivalent to factoring*, Springer, Berlin, 59-71, (1998).
5. D.J. Bernstein, J. Buchmann, and E. Dahmen (Eds.), *Post-Quantum Cryptography.* Springer, Berlin, 1-22, (2009).
6. W. Diffie and M.E. Hellman.,*New directions in cryptography.* IEEE Trans. Inf. Theory, IT-22, 6 , 644-654, (1976).
7. M. Hildebrand., *A survey on the mixing time of random walks on groups.*Markov Chains and Mixing Times, 2nd ed. American Mathematical Society, (2017).
8. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, and C. Park.*New public-key cryptosystem using braid groups.*, Springer, Berlin, 166-183, (2000).
9. N. Koblitz.,*Elliptic curve cryptosystems.* Math. Comput., 48, 177, 203-209, (1987).

10. H. Krawczyk and P. Eronen., *HKDF: A cryptographic key derivation function based on HMAC.* IETF RFC 5869, (2010).

11. J.C. Lagarias (Ed.).,*The Ultimate Challenge: The 3x+1 Problem.* American Mathematical Society, Providence, RI, (2010)

12. E. Lubetzky and Y. Peres., *Cutoff on all Ramanujan graphs.* Geom. Funct. Anal., 26, 1190-1216, (2016).

13. R. Mallikarjuna and B. Pushpalatha., *A symmetric cryptographic algorithm using a modified Collatz function.* Int. J. Comput. Appl., 92, 17, 1-7, (2014).

14. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone.*Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL, (1996).

15. R.C. Merkle.,*Secure communications over insecure channels.* Commun. ACM., 21, 4, 294-299, (1978).

16. V.S. Miller., *Use of elliptic curves in cryptography*, Springer, Berlin, 417-426, (1986).

17. B. Pushpalatha and P.K. Srimani.,*Secure key exchange using Collatz-like problem.* Int. J. Comput. Appl.,52, 3, 1-6, (2012).

18. O. Regev., *On lattices, learning with errors, random linear codes, and cryptography.* J. ACM, 56, 6, 1-40, (2009).

19. A. Rukhin et al., *A statistical test suite for random and pseudorandom number generators for cryptographic applications.* NIST Special Publication 800-22, (2010).

20. P.K. Srimani and B. Pushpalatha., *A new public key cryptosystem based on the Collatz problem.* Int. J. Netw. Secur. Appl., 5, 4, 1-10, (2013).

21. W. Stallings., *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, London, (2017).

22. H.R. Vidyashree and S. Lakshminarayana., *Visualizing and proving the Collatz conjecture: An Ananta-graph approach.* Commun. Appl. Nonlinear Anal., 32, 6s, 16-25, (2025).

23. H.R. Vidyashree and S. Lakshminarayana., *Symmetric key encryption using modular traversal of Ananta-graphs.* J. Inf. Syst. Eng. Manage. 10, 44s, 823-831, (2025).

Vidyashree H. R.,
Department of Mathematics,
REVA University,
Bangalore, Karnataka, India.
E-mail address: vidyashree848@gmail.com

and

Nagu Vadlana,
Department of CSE,
IIITDM Kurnool,
Andhra Pradesh, India.
E-mail address: vadlananagu95@gmail.com

and

Lakshminarayana S.,
Department of Mathematics,
REVA University,
Bangalore, Karnataka, India.
E-mail address: narayana_s@reva.edu.in