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

(3s.) **v. 2026 (44) 2** : 1–9.
ISSN-0037-8712
doi:10.5269/bspm.80462

Graph Coloring - Based Approach to Secure Shamir's Secret Sharing

Renuka Lakshmi A., S. Ramalingeswara Rao,Venkata Ramana P. and G. B. Chandra Mouli

ABSTRACT: This paper introduces a graph coloring–based enhancement of Shamir's Secret Sharing (SSS) to strengthen the security of distributed secret distribution. In the proposed method, participants are represented as vertices in a graph, and coloring constraints ensure that adjacent participants do not receive complementary share information, thereby minimizing the risk of collusion and data leakage. The results show that the scheme enhances robustness and access control while preserving the computational efficiency of traditional SSS.

Keywords: Graph coloring, chromatic polynomial, Interpolation polynomial, Shamir's secret sharing, cryptography.

Contents

2020 *Mathematics Subject Classification:* 94A62, 05C15, 05C31, 41A05.
Submitted November 29, 2025. Published March 14, 2026

1. Introduction

In 1979, Shamir and Blakley [11 & 12] introduced the concept of secret sharing through threshold schemes, using polynomials and finite geometries as the foundation. Since then, numerous researchers have expanded upon this basic threshold scheme concept, incorporating various mathematical structures to adapt the model for practical applications [1,3,4]. This paper builds on Shamir's original construction and demonstrates how it can be applied to develop these adapted models. Specifically, the authors present new constructions for multipart, multilevel, democratic, and prepositioned schemes. Additionally, they show how established methods for detecting cheaters and disenrolling participants can be integrated into Shamir's framework. Shamir's Secret Sharing (SSS) is a well-established cryptographic protocol that enables a secret to be distributed among multiple participants in such a way that the secret can only be reconstructed when a sufficient number of participants collaborate. The secret is divided into shares using a polynomial of degree t-1, where t is the threshold number of shares required to reconstruct the secret. Any subset of t or more participants can combine their shares to recover the secret, while fewer than t participants gain no information.

1.1. Brief Overview of Secret Sharing

Secret sharing is a technique used to distribute a secret (such as a cryptographic key or a password) among multiple participants (or nodes) so that only authorized subsets of participants can reconstruct the original secret. A commonly known secret sharing scheme is Shamir's Secret Sharing. Secret sharing is crucial in various fields such as secure communication, distributed systems, and multi-party computation, ensuring that no single party has full control over the secret [3].

1.2. Current Security Concerns in Secret Sharing

Traditional secret-sharing schemes face several potential vulnerabilities. Data leakage occurs when a participant or adversary gains access to part of the secret and attempts to infer or exploit other shares [2, 3]. Collusion is another risk, where unauthorized participants combine their shares to reconstruct the secret [2, 3]. Additionally, replay attacks may arise when malicious participants reuse shares in unintended ways to compromise the system [2, 3].

1.3. Introduce Graph Coloring

Graph coloring is a technique used to assign labels (colors) to the vertices of a graph so that no two adjacent vertices share the same color. This ensures that adjacent nodes are distinguishable, which is useful in many applications such as scheduling problems or resource allocation [9, 14]. In the context of secret sharing, the graph represents participants (nodes), and the edges represent potential access or relationships between these participants [4].

1.4. Using Graph Coloring for Secure Access Control

Now, begin connecting graph coloring with secret sharing, using, you can think of each participant in a secret-sharing scheme as a node in a graph. The edges between nodes represent relationships or dependencies, like trust or communication channels between participants. By coloring the graph, you ensure that sensitive secrets are shared in a way that minimizes the risk of malicious actors (those who hold specific colored shares) being able to reconstruct the secret without sufficient trust or collaboration.

1.5. Improving Security with Graph Coloring

By assigning colors to participants, access to the secret can be restricted based on the color configuration. For example, adjacent nodes (participants) may not be allowed to share certain portions of the secret if they share the same color, creating a more complex structure for valid reconstruction in which only specific configurations of participants with distinct colors can collaborate to reveal the secret [1, 4, 6]. Careful graph coloring also helps prevent unauthorized collusion; if participants that are close to each other in the graph (i.e., connected by an edge) have different colors, colluding participants cannot easily combine their shares to reconstruct the secret. Moreover, graph coloring enhances redundancy and fault tolerance by distributing secrets across nodes so that even if a few participants are compromised, the overall system can still function securely. The use of graph coloring adds complexity to the system,

making it harder for unauthorized participants to infer or reconstruct the secret. By designing secret-sharing systems based on graph theory, you can more easily control and enforce security policies in a fine-grained manner. Despite its robust security in terms of threshold-based reconstruction, SSS does not inherently address certain risks such as collusion or the leakage of information when participants have complementary knowledge. These concerns arise in distributed systems where multiple participants may share a common goal or adversarial intent. To mitigate such risks, graph coloring techniques offer an innovative approach for enhancing the distribution of shares in SSS. The combination of SSS and graph coloring introduces a layer of structural security that strengthens the scheme by controlling how shares are distributed across participants. This approach enables a more secure and efficient implementation of secret sharing, particularly in scenarios where participant interaction needs to be carefully managed to avoid potential vulnerabilities.

2. Materials

2.1. Shamir's secret sharing Goal

Consider a central authority P that holds a secret sss (a natural number) [11]. The objective is to distribute this secret among n participants $(P_1, P_2, ..., P_n)$ so that no individual participant can recover 's' on their own. At the same time, the scheme guarantees that any qualified subset of at least two participants can collaboratively combine their shares to fully reconstruct the original secret s.

2.2. Sharing Algorithm

It's based on the idea that t points uniquely determine a polynomial of degree t-1. The secret is embedded as the constant term of such a polynomial.

- Define a secret: Let the secret be s, an integer.
- Set the threshold: Choose a threshold t (minimum number of shares to reconstruct).
- Select the total shares: Choose total number of shares n, where $n \geq t$.
- Pick a prime modulus: Choose a prime number $p > \max(s, n)$.
- Form the polynomial: Construct a random polynomial $f(x)$ of degree $t-1$ such that

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \mod p,$$

where $a_0 = s$ is the secret and $(a_1, \cdots, a_{t-1})$ are random coefficients in the field $\mathbb{Z}_p$.

2.3. Share Distribution

- Compute the polynomial values at each participant's index:

$$f(1), f(2), ..., f(n)$$

- Assign each participant a share in the form of a pair:

$$(x_i, f(x_i))$$

where x_i is the participant's index and $f(x_i)$ is the corresponding polynomial value.

2.4. Reconstruction

- Any group of t or more participants can combine their shares to reconstruct the polynomial f(x).
- Using Lagrange interpolation, compute f(x), and then evaluate f(0) to retrieve the secret s

2.5. Definition of Chromatic polynomial

For a graph G, the chromatic polynomial $P_G(k)$ represents the number of proper vertex colorings of G using k distinct colors [7, 8 & 13].

2.6. Construction of chromatic polynomial of a graph G

A recursive method known as the deletion– contraction method, which is based on simplifying the graph step by step

2.6.1 Deletion–Contraction Method

Let G be a graph and e an edge in G. Then the chromatic polynomial satisfies the relation:

$$P_G(k) = P_{G-e}(k) - P_{G/e}(k)$$

where:

- $G - e$: the graph with edge e deleted (vertices remain unchanged).
- G/e: the graph with edge e contracted (the endpoints of e are merged).
- k: the number of available colors [10,13 & 14].

2.6.2 Step-by-step construction of the deletion–contraction method

- Step 1: Choose an edge e that is not a loop.
- Step 2: Apply the formula
$$P_G(k) = P_{G-e}(k) - P_{G/e}(k)$$
which is the standard deletion–contraction relation for the chromatic polynomial.
- Step 3: Repeat recursively for each of the resulting graphs until all edges are gone.
- Step 4: Base cases
  - Empty graph: if G has no edges and n vertices,
$$P_G(k) = k^n.$$
Each vertex can be any color since there are no edge constraints.
  - Complete graph K_n:
$$P_{K_n}(k) = k(k-1)(k-2)\cdots(k-n+1).$$
  - Tree with n vertices:
$$P_{\text{tree}}(k) = k(k-1)^{n-1}.$$
  - Cycle graph C_n:
$$P_{C_n}(k) = (k-1)^n + (-1)^n(k-1).$$

3. Methodology

Approaches to Secret Sharing and Chromatic Polynomials

3.1. Interpolation and Polynomial Reconstruction

In both secret sharing and chromatic polynomial analysis, determining a polynomial from a set of points or constraints is a central task.

- **Shamir's Secret Sharing (SSS):** Given share values (x_i, y_i), polynomial interpolation (usually Lagrange interpolation) is used to reconstruct the secret, which is the constant term of the polynomial.
- **Chromatic Polynomials:** Evaluating $P_G(k)$ at specific integer values $k = 1, 2, \ldots$ allows reconstruction of the polynomial from these known values. Thus, interpolation techniques such as Lagrange interpolation can be applied to reconstruct chromatic polynomials from evaluations:
$$P_G(k) = \sum_i y_i \, \ell_i(k),$$
where $\ell_i(k)$ are the Lagrange basis polynomials corresponding to the known points (k_i, y_i).

3.2. Modular Arithmetic and Finite Fields

Shamir's Secret Sharing (SSS) operates over finite fields to ensure secure and well-defined arithmetic operations. Certain graph-coloring problems also reduce to computations over finite fields (for example, testing 2-colorability using $\mathbb{F}_2$), although chromatic polynomials are classically defined over $\mathbb{Z}$.

3.3. Encoding Discrete Structures

Both SSS and chromatic polynomials encode discrete constraints into polynomial form:

- The chromatic polynomial encodes the constraint that *adjacent vertices must receive distinct colors.*
- SSS encodes the requirement that only authorized subsets of shares can reconstruct the secret.

3.4. Algebraic Combinatorics and Matroids

In advanced algebraic combinatorics, matroids generalize both graph coloring properties and polynomial interpolation structures. Thus, matroid theory provides a higher-level conceptual bridge between these two areas.

3.5. Theoretical Connection via Interpolation

A chromatic polynomial can be conceptualized through its values at selected points $k_1, k_2, \ldots, k_n$. Once these evaluations are known, one may apply Lagrange interpolation to reconstruct the full polynomial.

If

$$P_G(k_i) = y_i \quad \text{for known points } (k_i, y_i),$$

then the chromatic polynomial can be expressed as

$$P_G(k) = \sum_i y_i \, \ell_i(k),$$

where $\ell_i(k)$ are the Lagrange basis polynomials determined by the points (k_i, y_i).

This provides a direct algebraic link between the evaluation-based reconstruction used in Shamir's Secret Sharing and the reconstruction of chromatic polynomials from known values.

3.6. Reconstruction of a Chromatic Polynomial Using Lagrange Interpolation

- Step 1: Choosing a Graph

  Consider the complete graph $G = K_4$ with 4 vertices and 6 edges.

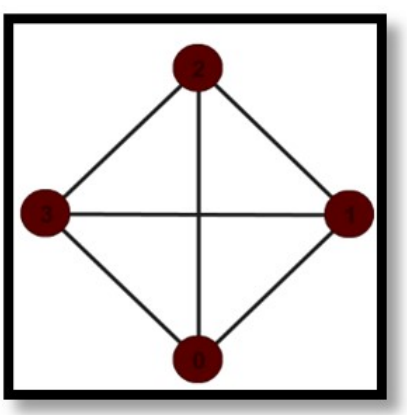

Figure 1: Graph used for chromatic polynomial reconstruction

- Step 2: Chromatic Polynomial of K_4

  The number of proper colorings with k colors is computed as follows:

  - Vertex v_1: k choices.
  - Vertex v_2: $k-1$ choices (different from v_1).
  - Vertex v_3: $k-2$ choices (different from v_1 and v_2).
  - Vertex v_4: $k-3$ choices (different from v_1, v_2, v_3).

  Thus,
  $$P_G(k) = k(k-1)(k-2)(k-3) = k^4 - 6k^3 + 11k^2 - 6k.$$

  For the purpose of interpolation-based reconstruction, we assume this formula is *unknown* and recover it using Lagrange interpolation.

- Step 3: Evaluating $P_G(k)$ at Specific Points

  The values of the chromatic polynomial at selected integers are:

k	$P_G(k) = k^4 - 6k^3 + 11k^2 - 6k$
1	0
2	0
3	0
4	24
5	120

  We now use Lagrange interpolation to find the degree-4 polynomial
  $$P_G(k) = a_4k^4 + a_3k^3 + a_2k^2 + a_1k + a_0$$
  that fits the data points $(k_i, P_G(k_i))$.

  The Lagrange form of the polynomial is:
  $$P_G(k) = \sum_{i=1}^{5} P_G(k_i)\,\ell_i(k),$$
  where each $\ell_i(k)$ is the Lagrange basis polynomial
  $$\ell_i(k) = \prod_{\substack{j=1 \\ j\neq i}}^{5} \frac{k-k_j}{k_i-k_j}.$$

- Step 4: Lagrange Interpolation Computation

  Let us compute each Lagrange basis polynomial.

  For $l_0(k)$ corresponding to the point $(1,0)$:
  $$l_0(k) = \frac{(k-2)(k-3)(k-4)(k-5)}{(-1)(-2)(-3)(-4)} = \frac{(k-2)(k-3)(k-4)(k-5)}{24}.$$

  For $l_1(k)$ corresponding to the point $(2,0)$:
  $$l_1(k) = \frac{(k-1)(k-3)(k-4)(k-5)}{(1)(-1)(-2)(-3)} = \frac{(k-1)(k-3)(k-4)(k-5)}{-6}.$$

For $l_2(k)$ corresponding to the point $(3, 0)$:

$$l_2(k) = \frac{(k-1)(k-2)(k-4)(k-5)}{(2)(1)(-1)(-2)} = \frac{(k-1)(k-2)(k-4)(k-5)}{4}.$$

For $l_3(k)$ corresponding to the point $(4, 24)$:

$$l_3(k) = \frac{(k-1)(k-2)(k-3)(k-5)}{(1)(2)(3)(-1)} = \frac{(k-1)(k-2)(k-3)(k-5)}{-6}.$$

For $l_4(k)$ corresponding to the point $(5, 120)$:

$$l_4(k) = \frac{(k-1)(k-2)(k-3)(k-4)}{(1)(2)(3)(1)} = \frac{(k-1)(k-2)(k-3)(k-4)}{6}.$$

Now compute the reconstructed polynomial:

$$P(k) = 0 \cdot l_0(k) + 0 \cdot l_1(k) + 0 \cdot l_2(k) + 24\, l_3(k) + 120\, l_4(k).$$

Thus,

$$P(k) = 24 \cdot \frac{(k-1)(k-2)(k-3)(k-5)}{-6} + 120 \cdot \frac{(k-1)(k-2)(k-3)(k-4)}{6}.$$

Simplifying gives:

$$P(k) = k^4 - 6k^3 + 11k^2 - 6k,$$

which is exactly the chromatic polynomial of K_4.

A chromatic polynomial is reconstructed from evaluations using Lagrange interpolation, same as Shamir's secret sharing reconstructs a polynomial to obtain the secret. Although they are not the same, this demonstrates how interpolation ties discrete combinatorics and secret sharing cryptography, both of which rely on the strength of polynomials together.

4. Results and Discussion

The integration of graph coloring techniques into Shamir's Secret Sharing (SSS) produced results that highlight both theoretical significance and practical applicability.

4.1. Secure Share Distribution

Modeling participants as graph vertices and assigning proper coloring constraints ensured that no two adjacent participants possessed complementary share information. This directly reduced the risk of collusion attacks, thereby enhancing the confidentiality and reliability of the secret-sharing process [1 & 4].

4.2. Algebraic Connection with Chromatic Polynomials

Through the example of the complete graph K4, the study demonstrated that chromatic polynomials can be reconstructed via Lagrange interpolation, in the same way that secrets are reconstructed in SSS. This establishes a strong algebraic parallel between interpolation in cryptography and graph coloring in combinatorics, offering a deeper theoretical foundation for the proposed scheme.

4.3. Strengthened Security and Robustness

The proposed method addresses vulnerabilities present in classical SSS, particularly data leakage and unauthorized collusion. By embedding graph coloring constraints into the share distribution process, stricter access control mechanisms were achieved, ensuring that only authorized participant configurations can reconstruct the secret.

4.4. Preservation of Computational Efficiency

Despite the introduction of graph coloring, the reconstruction process continues to rely on Lagrange interpolation, which preserves the efficiency of the original SSS scheme. This confirms that the enhanced structure does not impose significant computational overhead while providing stronger security guarantees.

4.5. Practical Relevance

The approach demonstrates high potential for real-world deployment in systems where resistance to collusion and fault tolerance are critical, including secure communication protocols, blockchain networks, and distributed cloud storage environments.

5. Conclusion

This work proposed a novel framework that integrates graph coloring with Shamir's Secret Sharing to enhance the security of distributed cryptographic systems. By combining combinatorial structures with polynomial interpolation, the approach effectively prevents collusion, mitigates risks of data leakage, and strengthens access control while maintaining the computational efficiency of traditional SSS. The established connection between chromatic polynomials and interpolation not only enriches the theoretical understanding of secret sharing but also provides a robust mathematical foundation for future advancements. The findings demonstrate that this integration can play a pivotal role in designing resilient protocols for secure communication, blockchain technology, and cloud-based data protection.

Future Scope

The proposed graph coloring–based framework for Shamir's Secret Sharing offers several promising research directions. One potential extension lies in adapting the scheme to advanced access structures such as hierarchical, multipart, or dynamic models, where participant roles and trust levels evolve over time. Exploring algorithmic optimizations for graph coloring in cryptographic contexts may also improve efficiency, making the scheme viable for real-time secure communication systems. In addition, testing the approach in large-scale distributed environments such as cloud storage, blockchain platforms, and multiparty computation protocols will provide valuable insights into its scalability and robustness. Empirical validation and integration with emerging technologies will not only strengthen the practical utility of the scheme but also contribute to the broader development of resilient and secure distributed systems.

References

1. D. Dafik, I. Firdausiyah, R. Adawiyah, I. H. Agustin, I. L. Mursyidah, and M. Marsidi, "Analysis of Rainbow Vertex Antimagic Coloring and its application in secret sharing and cryptography," *Jurnal Teori dan Aplikasi Matematika*, 2025.
2. D. Gomathi and S. Nagarajan, "An ASCII Value Based Data Encryption Using Coloring Tripartite Graph," *Contemporary Mathematics*, 2025.
3. A. Meenakshi, S. Dhanushiya, L. Mrsic, A. Kalampakas, and S. Samanta, "A multi layered encryption framework using intuitionistic fuzzy graphs and graph theoretic domination for secure communication networks," *Scientific Reports*, vol. 15, Article 20992, 2025.
4. R. M. Falcon, K. Abirami, N. Mohanapriya, and Dafik, "Enhancing Data Security through Rainbow Antimagic Graph Coloring for Secret-Share Distribution and Reconstruction," *arXiv*, 2024.
5. T. Nian, S. Tsujie, R. Uchiumi, and M. Yoshinaga, "qqq-deformation of chromatic polynomials and graphical arrangements," *arXiv*, 2024.
6. R. Sazdanovic and D. Scofield, "Structure of the chromatic polynomial," *arXiv*, 2024.
7. T. Gayathri and S. Govindan, "Chromatic Polynomial of Graphs," *Aut Aut Research Journal*, Oct. 2020, pp. 40–46.
8. B. R. Srinivas, "Chromatic polynomials," *International Journal of Scientific and Innovative Mathematical Research (IJSIMR)*, vol. 2, no. 11, pp. 918–920, 2014.
9. G. Chartrand, *Chromatic Graph Theory*, Taylor & Francis Group, USA, 2009, pp. 14–167.
10. T. H. Tamás, "The chromatic polynomials," *Eötvös Loránd University Journal*, vol. 12, pp. 12–18, 2009.
11. A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

12. G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS 1979 National Computer Conference*, vol. 48, pp. 313–317, New York, 1979.

13. R. C. Read, "An Introduction to Chromatic Polynomials," *Journal of Combinatorial Theory*, vol. 4, pp. 52–71, 1968.

14. H. Whitney, "The Coloring of Graphs," *Annals of Mathematics*, vol. 33, pp. 688–718, 1932.

Renuka Lakshmi A.,
Department of Mathematics,
Vasireddy Venkatadri International Technological University,Nambur
India.
E-mail address: renukalakshmiavvari@vvit.net

and

S. Ramalingeswara Rao,
E.M& H Department,
SRKR ENGINEERING COLLEGE,BHIMAVARAM
India.
E-mail address: renukalakshmiavvari@vvit.net, ramu.eswar30@gmail.com

and

Venkata Ramana P.,
Department of Mathematics,
Vasireddy Venkatadri International Technological University,Nambur
India.
E-mail address: paladuguvenkataramana@gmail.com

and

G. B. Chandra Mouli,
Department of Mathematics,
Aditya Univeristy, Surmapalem,
India.
E-mail address: gbchandramouli@gmail.com