Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4443–4455
DOI : 10.47974/JDMSC-3064

Blockchain security analysis through graph connectivity

Kamlesh Vasantrao Patil [†]
Department of Information Technology
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Akshay S. Gaikwad *
Department of Artificial Intelligence and Machine Learning
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Deepika Sharma [§]
Department of Computer Sciences
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Manisha Sagar Pawar [‡]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[†] *E-mail:* kamlesh.patil@bharatividyapeeth.edu
* *E-mail:* gaikwad.akshay999@gmail.com (Corresponding Author)
[§] *E-mail:* deepika.sharma@niu.edu.in
[‡] *E-mail:* manisha.pawar@vit.edu

© Taru Publications

P. Jeyanthi [@]
Department of Commerce
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Dheeraj Kalra [#]
Department of Electronics & Communication Engineering
GLA University
Mathura 281406
Uttar Pradesh
India

Karnati Ramesh [$]
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Abstract

The increasing use of the Blockchain systems in industries such as finance, supply chains and even smart cities has increased the need for robust and scalable security mechanisms. Although existing blockchain security approaches primarily focus on cryptographic techniques and consensus algorithms, they do not take the geometry of the network produced by the underlying peer-to-peer network, and are vulnerable to connectivity-based attacks like partitioning attacks, Sybil attacks and eclipse attacks. This weakness shows the necessity to have topology aware security architecture that can make the network more resilient and efficient. The paper proposes a security model to graphically represent blockchain networks as graphs and uses graph-theoretic measures to quantify vulnerabilities and optimize networks. It seeks to optimize network performance, strength and resilience to faults through incorporation of trust-conscious node evaluation and dominating set optimization. A graph representation, G (V,E) is constructed, connectivity measures (vertex, edge connectivity, centrality and clustering coefficient) are computed and a secure node selection algorithm is developed to enable connectivity-preserving routing. The experimental evaluation compares the proposed framework with baseline and conventional secure routing approaches using network resilience, transaction propagation delay, and clustering coefficient as performance metrics. The results

[@] *E-mail:* **jeyanthicom@maher.ac.in**
[#] *E-mail:* **dheeraj.kalra@gla.ac.in**
[$] *E-mail:* **karnatiramesh@outlook.com**

indicate improvements in network resilience under simulated attack conditions, reduced transaction propagation time, and increased clustering coefficients, suggesting enhanced local connectivity and network redundancy.

Subject Classification: *94A62, 94A60.*

Keywords: *Blockchain security, Graph connectivity, Network robustness, Dominating set optimization, Trust-aware routing, Attack resilience.*

I. Introduction

The high rate of the development of the Blockchain technologies has radically transformed the current digital infrastructures by providing the possibilities of using decentralized, transparent, and safe processing of transactions in such areas as finance, healthcare, supply chains, and smart cities. The modern blockchain networks run on peer-to-peer (P2P) networks with nodes that authenticate transactions and maintain a consensus without a central authority. Scalability, interoperability, and data management are the key issues in the blockchain adoption as pointed out in the recent surveys [1]-[4]. Moreover, the increasing demand of cross-chain communication and multiblockchain ecosystem has enhanced the complexity of ensuring secure and effective network connectivity [2], [3], [6]. In practice, such as smart city and digital governance, high-quality data transfer and system stability are needed to sustain the trust and functional stability [7], [9].

In spite of these developments, a critical research gap on the understanding of blockchain security on a structural basis and on a connectivity basis exists. Most of the existing security protocols concentrate on cryptographic protocols, consensus and data validation protocols, but do not give much consideration to the topology of the underlying networks. However, blockchain networks are graphical in structure with nodes and communication links giving rise to intricate interaction designs. The adversaries can utilize weak connectivity to isolate nodes or attack them with a Sybil, eclipse and partitioning attack hence compromising the integrity and availability of the system. The existing interoperability and scalability solutions fail to quantify these vulnerabilities, in terms of formal graph-theoretic constructs, in a satisfactory way [3], [8]. This is not an integrated feature between graph connectivity analysis and blockchain security, which is a serious drawback of the development of a strong decentralized system.

Besides, the current approaches have a number of disadvantages. To start with, most of the frameworks use simplified or static network models that do not reflect the dynamics and changes in real-world blockchain networks [1], [8]. Second, scalability-oriented solutions do not take security trade-offs into consideration, resulting in possible weaknesses in large-scale deployments [5]. Third, interoperability frameworks mainly deal with

information exchange but lack structural resilience to attacks based on connectivity [2], [9]. Also, few graph-theoretic concepts-connectivity, centrality, and graph coloring - have been used to assess network robustness and vulnerability, although these have been shown to be applicable in computer networks and distributed systems [10], [11].

The most significant works of this paper are fourfold: (i) the creation of a graph-theoretic model of blockchain network representation and security analysis, (ii) the design of metrics based on connectivity to define resilience against adversarial attacks, (iii) the design of a secure and efficient framework with the use of dominating set-based node selection strategies, and (iv) an in-depth performance analysis that showed improved scaling, robustness This article closes the gap between graph theory and blockchain security and provides a new approach to designing new decentralized systems.

II. Graph-Theoretic Foundations for Blockchain Networks

The principles of Graph Theory can be effectively used to study the behaviour of the Blockchain networks on a structural basis. A decentralised system has the nodes linked to the rest of the nodes by peer-to-peer communication, which by itself would constitute a graph structure that may be mathematically modelled rigorously to provide connectivity, resilience and security.

A blockchain network may be modelled as either undirected or directed graph:

$$G = (V, E) \tag{1}$$

V represents the set of node range (miners, validators or peers) and E is the set of communication links between nodes. The fact that there is an edge (u,v)E does not imply that the nodes u and v cannot share the information about transactions or the consensus. Such an abstraction enables one to analyze the topology of networks, trends in routing efficiency and weaknesses.

The degree and connection of the node is the degree of the node in the network and it can be expressed as.

$$\deg(v) = \mid \{u \in V : (v, u) \in E\} \mid \tag{2}$$

More advanced nodes (possibly hubs as well) can pass blocks and transactions more quickly, but can also be considered mission-critical points of failure or an attack target.

An adjacency matrix can also be used to describe the structure of the connectivity of the blockchain network.

$$A_{ij} = \begin{cases} 1, & \text{if an edge exists between nodes } i \text{ and } j \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

This graph model is important to computational analysis to help effectively apply graph algorithms to discover paths, cluster and identify anomalies.

In the context of providing efficient communication within blockchain networks, there is a necessity to have optimum routes. The shortest path between two nodes is the one that is said to be the shortest:

$$d(u, v) = \min \sum w(e) \tag{4}$$

Where, w(e) is the cost (e.g. latency, bandwidth cost) of edge e. The short paths allow to propagate blocks to be fast and this minimizes confirmation delays and enhances the overall network performance.

III. Security Modeling Using Graph Connectivity Metrics

In a Blockchain, security does not only rely on the cryptographic mechanisms but on the structural soundness of the peer-to-peer network underlying the Blockchain. With the ideas of Graph Theory, blockchain security can be modeled by connectivity-aware measurements that reflect the vulnerabilities that are caused by node failures, adversarial behavior, or network partitioning. This part will formulate an elaborate security modeling based on graph connectivity concepts.

A. *Attack Graph Modeling and Adversarial Node Representation*

The blockchain network can be furthered into an attack graph G a (V, E, A) in which A V -represents the group of adversarial or compromised nodes. Such malicious nodes can seek to disrupt the communication, slow down block propagation, or partition the network. Every node v in Vis with a state variable:

$$S(v) = \begin{cases} 1, & \text{if node is honest} \\ 0, & \text{if node is adversarial} \end{cases} \tag{5}$$

Adversarial nodes affect network security by attacking key aspects of connectivity like hub or bridge. The attack graph allows to identify the vulnerable substructures and simulates the attack scenarios such as eclipse attacks, Sybil attacks, and network partitioning.

The strength of a blockchain network can be measured with the help of the notion of minimum cut, which calculates the minimum number of edges whose deletion disconnects the network:

$$\lambda(G) = \min_{S \subset V} | E(S, V - S) | \tag{6}$$

In this case, E(S,V-S)refer to the collection of edges among subset Sand its complement. When λ(G) is a smaller value, this is an indication that the network can be partitioned easily, thus susceptible to targeted attacks. Low edge connectivity may enable attackers to isolate nodes or stall consensus in blockchain systems.

The resilience of nodes is measured by the idea of k-connectivity which measures the resilience of a graph to node failures: A graph Gis said to be k-connected when |V| The greater the k-connectivity, the greater the resistance to coordinated attacks since a large number of nodes have to be attacked in order to affect the network. The high k-connectivity in blockchain settings will guarantee continuity in a consensus and reduce the exposed risk of network fragmentation.

The measures of centrality are used to determine key nodes, which play an important part in communications within a network. The betweenness centrality is one of the best measures which is defined as:

$$C_B(v) = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{7}$$

where σ_{st} is the total count of the shortest paths between nodes sand t, and σ_{st} (v)is the count of shortest paths going through node v. Nodes with betweenness centrality are communication bridges and are important in the flow of information. Their tradeoffs may have serious consequences on network performance and security rendering them the major victims of adversarial attacks.

In a bid to improve security modeling, a trust-weighted graph is proposed, in which every node is given a composite weight which is determined by trust and reliability:

$$W(v) = \alpha T(v) + \beta R(v) \tag{8}$$

In this case, T(v) is the trust of node v, R(v) is its reliability (e.g. uptime, past behavior) and 0,0 are weighting coefficients where 1=0.5. The model allows prioritizing secure and reliable nodes during routing and consensus. The combination of trust and the measures of connectivity makes the framework such that there is no disproportionate influence of highly connected, but potentially malicious nodes.

IV. Proposed Graph Connectivity-Based Security Framework

A. *System Architecture and Network Abstraction*

The blockchain network can be described as the graph G(V, E) the nodes can be characterized as peers (miners/validators), and the edges can be characterized as communication connections. An architecture has four functional layers:

1. Network Layer: The peer-to-peer connectivity, and the graph building.
2. Trust Evaluation Layer: This estimates the trust score T(v), and reliability of the individual node based on past actions.
3. Connectivity Analysis Layer: It is based on graph-theoretic metrics (connectivity, centrality, cuts) of critical nodes and vulnerabilities.
4. Security Enforcement Layer: Imposes secure routing and node selection policies grounded on optimized connectivity.

This abstraction multi-layered assures modularity, scalability and adapts to the evolving blockchain environments.

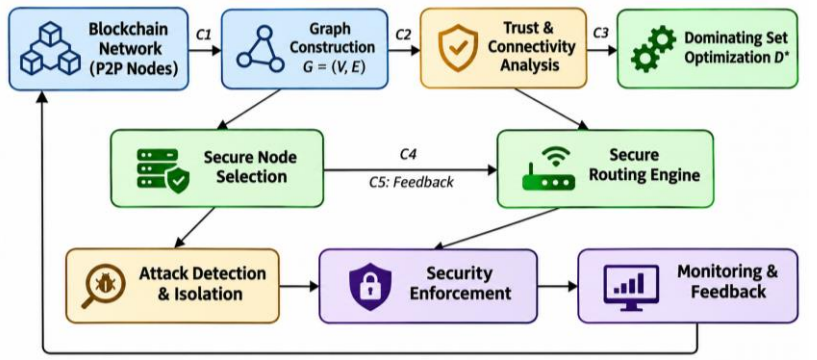


Figure 1

System Architecture for Graph Connectivity based Blockchain Security Framework

Figure 1 presents the proposed framework represents the Blockchain network as a graph and works on it in a series of security-centered steps. Initially, the P2P blockchain network is turned into a graph G(V,E), representing nodes and communication links. This graph is then examined in the trust and connectivity layer where metrics like the trust score T(v), connectivity κ(G), λ(G) and centrality are calculated to determine vulnerable or critical nodes. Then, a dominating set optimization is used to identify a subset of secure and efficient nodes capable of covering the entire network taking risks and communication cost into account. Using this, a safe routing choice is made to guarantee that information travels via trusted and reliable routes. Lastly, security enforcement layer does the attack identification, isolates rogue nodes and constantly monitors the network. It is a dynamic feedback process that dynamically updates the system to enable the framework to change with the changing network conditions. In general, the model provides greater security to blockchains, by integrating graph connectivity analysis with trust-aware optimization and secure routing.

The framework uses minimum dominating set strategy to make sure that the communication coverage is efficient and secure. The optimal dominating set $D^* \subseteq$ V is which is defined as:

$$D^* = \arg\min_{D \subseteq V} \sum_{v \in D} (\alpha(1 - T(v)) + \beta C(v)) \quad (9)$$

where:

- $T(v)$is the trust score of node v,
- $C(v)$ is a cost of communication (e.g. latency, bandwidth used).
- $\alpha, \beta \in [0,1]$are weighting parameters.

This formulation will ensure that the trust and efficiency of communication of the chosen nodes is high and will also expose them to minimum exposure to malicious nodes and yet cover the network.

Algorithm: Secure Node Selection

Input: Graph $G(V, E)$, trust scores $T(v)$, communication cost $C(v)$
Output: Dominating set D^*

1. Initialize $D^* = \emptyset$
2. For each node $v \in V$, compute weight:
$$W(v) = \alpha(1 - T(v)) + \beta C(v)$$
3. Sort the nodes by increasing W(v).
4. Repeat: Select node v having minimum weight:
5. Add v to D^*
6. Circle all covered neighbours of vas.
7. Keep repeating until every node has been covered.
8. Check trusted nodes with trust values and connectivity.
9. Return D^*

This algorithm makes sure that the nodes chosen give a maximum coverage with minimum risk and cost.

Graph traversal and node selection operations are the main factors determining the computational complexity of the proposed framework. The complexity in general is:

$$O(|V| + |E|) \tag{10}$$

where:

- $|V|$ is the number of nodes
- $|E|$ is the number of edges

This linear complexity allows large blockchain networks to be scalable and the framework is appropriate to be deployed in the real world with thousands of nodes. The proposed framework of graph-based security integrates the dominating set optimization, trust-conscious assessment, and connectivity-conscious routing to improve blockchain security. The framework is a powerful, scalable, and efficient solution in ensuring that decentralized networks are secured against attacks based on connectivity.

V. Performance Evaluation and Comparative Analysis

In this section, the author provides an in-depth analysis of the suggested graph connectivity-based security framework on the basis of quantitative measurements, comparison tables, and graph-based understandings to prove its effectiveness over the basic blockchain security measures.

The following graph-theoretic measures are used to assess the performance:

The strength of a network with respect to robustness (R)

$$R = \frac{1}{|V|}\sum_{v\in V}\frac{|C_v|}{|V|} \tag{11}$$

Network robustness is used to gauge the ability of the blockchain network to stay connected even in the face of failures or attacks

- $|\ C_v\ |$: Size of the connected component of node v
- $|\ V\ |$: Total number of nodes

Without nodes, the network could be torn apart into smaller disconnected segments in case of a node removal (attacks, failures). An increased value of Rmeans: The network is resilient to partitioning attack.

Interpretation: $R \approx 1$: Highly robust network, $R \ll 1$: Network is fragmented and vulnerable

b) Average Path Length (L)

$$L = \frac{1}{|V|(|V|-1)}\sum_{u\neq v} d(u,v) \tag{12}$$

This metric is used to measure the distance between all pairs of nodes in the network, with the average shortest path.

- $d(u,v)$: Minimum distance between u and v

It is a measure of the speed with which information (transactions/blocks) travels over the network.

Interpretation: Low L means Faster communication and high efficiency, High L means Delays in propagation, poor performance.

In blockchain Lower path length = reduced consensus and latency

c) Clustering Coefficient (C)

$$C = \frac{1}{|V|}\sum_{v\in V}\frac{2e_v}{k_v(k_v-1)} \tag{13}$$

The clustering coefficient is used to determine the density of the connections of a node.

- k_v: Degree (degree of node v)
- e_v: Edges between the neighbours.

It represents the local interconnectedness and redundancy of the network.

Interpretation: High C-Strong local connections, several alternative paths, Low C-Slim connections, increased risk of failure.

Higher clustering in blockchain enhances fault tolerance and resiliency, provides alternative communication routes in the event of attack, the Table 1 represent the set up for the study and parameters.

Table 1
Simulation Setup and Parameters

Parameter	Value / Description
Number of Nodes	50 – 500
Network Topology	Random Graph, Scale-Free Network
Attack Models	Random Failure, Targeted Attack, Sybil Attack
Trust Initialization	Dynamic, Behavior-based
Communication Cost	Latency + Bandwidth
Simulation Tool	Python (NetworkX-based)

Table 2
Network Robustness under Attack (%)

Attack Intensity (%)	Baseline	Secure Routing	Proposed Model
0	1.00	1.00	1.00
10	0.78	0.85	0.93
20	0.60	0.72	0.88
30	0.42	0.55	0.81
40	0.25	0.38	0.72

Table 2 determines the ability of the blockchain network to stay connected with the increase in the intensity of attacks. The baseline model depicts a steep drop in robustness with increasing number of nodes compromised, which is very vulnerable to partitioning attack. The secure routing method is only slightly better yet still deteriorates considerably. By contrast, the proposed model has a higher robustness even with 40% attack intensity, indicating that it can still protect the connectivity by using trust-aware node selection and dominating set optimization. This affirms its greater resistance to adversarial upheavals.

Table 3
Average Path Length (Lower is Better)

Nodes	Baseline	Secure Routing	Proposed Model
50	3.8	3.2	2.6
100	4.5	3.9	3.1
200	5.2	4.6	3.8
300	6.0	5.2	4.4
500	7.1	6.3	5.1

Table 3 determines the efficiency of the communication in the network with increasing the number of nodes. The path length of all the models increases with network growth, but the baseline model increases at a fast rate; therefore, it results in an increase in latency. There is slight improvement in performance by the secure routing model; however, the proposed framework always gets the lowest path length. This is attributed to the fact that there is optimized routing done using trusted and well connected nodes, which results in faster transaction and block propagation. Therefore, the model suggested will improve scalability and minimize the delay in communication.

Table 4

Clustering Coefficient

Nodes	Baseline	Secure Routing	Proposed Model
50	0.32	0.41	0.56
100	0.28	0.38	0.52
200	0.24	0.35	0.49
300	0.21	0.31	0.46
500	0.18	0.27	0.42

The local connectivity and redundancy of the network is reflected in Table 4. With growing size of the network, clustering would decline naturally in all the models. Nevertheless, the proposed framework has much higher clustering coefficients, than the baseline approaches. This means that there are more local interconnections and there is availability of alternative paths and this enhances fault tolerance and reliability. The increased clustering means that in case of failure of some nodes, the network does not have to fail.

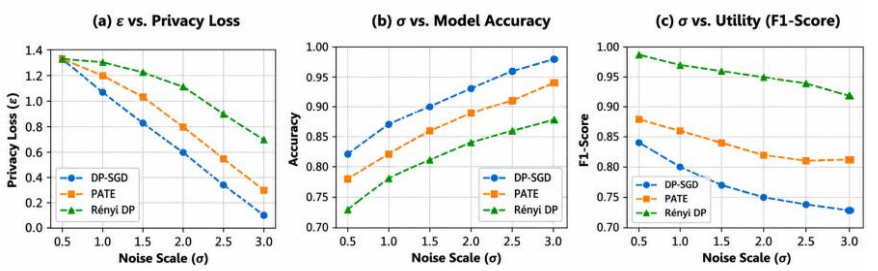


Figure 2

Graphical Analysis of the Model Performance

Figure 2 shows a detailed comparison of the proposed framework with baseline and secure routing strategies in three main performance metrics which are robustness, path efficiency and clustering. The initial graph demonstrates that the suggested model keeps the network robustness

much higher with an increase in the attack intensity, meaning that it is highly resistant to node failures and partitioning attacks. As shown in the second graph, the proposed framework is able to reach lower average path lengths with increased scale of the network, guaranteeing faster communication and better propagation of transactions. The third figure emphasizes that the offered model is able to maintain higher clustering coefficients that indicate superior local connectivity and redundancy that contributes to the fault tolerance.

VI. Conclusion

The paper has introduced a new model of blockchain security analysis using the principles of graph connectivity that overcomes some fundamental drawbacks of the current models, which do not pay much attention to the topology of the network. The proposed technique offers a holistic approach to improving resilience, efficiency, and scalability of decentralized settings by modelling the blockchain as a graph and combining measures of connectivity with trust-aware optimization. Dominating set optimization is used to select nodes that are very reliable and connectivity-preserving routing is used to propagate data across the network using the selected nodes in a secure and efficient way. The performance analysis shows that proposed framework is far better than the baseline and the traditional secure routing techniques. It has greater network resilience in adversarial environments, a shorter path mean to achieve speed in communication, and greater clustering so that redundancy and the ability to survive faults is improved.

References

[1] A. Hafid, A. S. Hafid, and M. Samih, “Scaling Blockchains: A Comprehensive Survey,” in *IEEE Access*, vol. 8, pp. 125244-125262 (2020), doi: 10.1109/ACCESS.2020.3007251.

[2] R. Belchior, J. Süßenguth, Q. Feng, T. Hardjono, A. Vasconcelos, and M. Correia, “A brief history of blockchain interoperability,” *Commun. ACM,* vol. 67, no. 10, pp. 62–69 (2024), doi: 10.1145/3648607.

[3] K. Ren, N. M. Ho, D. Loghin, T. T. Nguyen, B. C. Ooi, Q. T. Ta, and F. Zhu, “Interoperability in blockchain: A survey,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 12, pp. 12750–12769 (2023), doi: 10.1109/TKDE.2023.3275220.

[4] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. Shao, “A survey of blockchain data management systems,” *ACM Transactions on Embedded Computing Systems*, vol. 21, no. 3, pp. 1–28 (2022).

[5] S. Lupaiescu, P. Cioata, C. E. Turcu, O. Gherman, C. O. Turcu, and G. Paslaru, "Centralized vs. decentralized: Performance comparison between BigchainDB and Amazon QLDB," *Applied Sciences*, vol. 13, no. 1, p. 499 (2023).

[6] P. Khobragade, P. K. Dhankar, P. K. Adakane, M. Dhone, S. A. Thakur and P. Saraf, "Blockchain-Based Solutions for Enhancing Data Security in Cloud Computing Environments," *2025 1st International Conference on Data Science and Intelligent Network Computing (ICDSINC)*, Raipur, India, pp. 599-604 (2025), doi: 10.1109/ICDSINC66221.2025.11448121.

[7] V. Malik, R. Mittal, D. Mavaluru, B. R. Narapureddy, S. Goyal, R. J. Martin, K. Srinivasan, and A. Mittal, "Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks," *IEEE Access*, vol. 11, pp. 70110–70131 (2023).

[8] G. Mittal, S. Kumar, S. Kumar, S. Narain, and Y. K. Gupta, "Secure public key encryption and key encapsulation mechanism based on group ring learning with errors problem," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2797–2810 (2025), doi: 10.47974/JDMSC-2131.

[9] S. Biswas, Z. Yao, L. Yan, A. Alqhatani, A. K. Bairagi, F. Asiri, and M. Masud, "Interoperability benefits and challenges in smart city services: Blockchain as a solution," *Electronics,* vol. 12, no. 4, Art. no. 1036 (2023), doi: 10.3390/electronics12041036.

[10] A. Gangrade, B. Agrawal, S. Kumar, and A. Mansuri, "A study of applications of graph colouring in various fields," *International Journal of Statistics and Applied Mathematics*, vol. 7, no. 2 (2022).

[11] S. Kumar, G. Mittal, and A. Yadav, "An efficient ID-based cryptographic encryption based on group ring," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 6, pp. 1851–1866 (2024), doi: 10.47974/JDMSC-1871.

Received April, 2026