

QUANTUM SECRET SHARING PROTOCOL SECURITY IN CLOUD ENVIRONMENT

Mr. Pravin Balu, Laxmi Narayan Pandit, Punna Shiva, Somaraju Sairam

Department of Computer Science and Engineering, Guru Nanak Institute of Technology (Affiliated to

JNTUH-Hyderabad), Ranga Reddy District-501506, Telangana, India

Guide: Mr. Pravin Balu B, Assistant Professor, Department of CSE, GNIT

Abstract—Quantum Secret Sharing (QSS) is a fundamental cryptographic primitive that distributes a secret among multiple participants using quantum information, ensuring that only authorized subsets can reconstruct the original secret. Conventional QSS protocols rely on fixed network topologies and require full participation of all shareholders, introducing significant limitations in scalability, flexibility, and resilience against adversarial threats. This paper proposes a novel QSS framework built upon a generic distributed quantum network adopting a threshold-based (t, n) scheme, permitting any t out of n players to collaboratively reconstruct the secret. The proposed protocol integrates a custom weighting system and a quantum variant of Dijkstra's algorithm to dynamically select the optimal subset of participants, enhancing routing efficiency and overall system performance. To strengthen user authentication and provide identity obfuscation against both classical and quantum adversaries, CRYSTALS-Kyber post-quantum cryptographic primitives are incorporated alongside SHA-256 hashing. The system architecture adopts a three-tier model comprising a client layer, a processing layer governed by a Central Authority, and a data/security layer with quantum-encrypted storage. Comprehensive security analysis demonstrates compliance with the extended CIA triad and resilience against eavesdropping, impersonation, and collusion attacks. Simulation results confirm that the proposed protocol outperforms traditional QSS models, achieving improved fault tolerance, authentication security, and practical deployability in cloud-based distributed environments.

Keywords—Quantum Secret Sharing, CRYSTALS-Kyber, Post-Quantum Cryptography, Dijkstra's Algorithm, Threshold Scheme, Cloud Security, Quantum Entanglement

1. INTRODUCTION

The rapid proliferation of cloud computing platforms and distributed network architectures has intensified the demand for cryptographic protocols capable of providing strong confidentiality guarantees against both classical and emerging quantum threats. Secret sharing, introduced independently by Blakley [1] and Shamir [2], forms the cornerstone of secure distributed computation by dividing a secret into shares such that only authorized subsets of participants can reconstruct the original information. However, as quantum computing advances—highlighted by Shor's polynomial-time algorithm for factoring [3]—classical secret sharing schemes based on number-theoretic hardness assumptions face existential vulnerabilities.

Quantum Secret Sharing (QSS) addresses this challenge by leveraging quantum entanglement, superposition, and measurement irreversibility to achieve information-theoretic security. Early QSS protocols proposed by Hillery et al. [8] demonstrated that GHZ-state-based entanglement could securely distribute secrets; however, these approaches assumed static network topologies and mandated full participation of all n shareholders, limiting adaptability in dynamic cloud environments.

The existing literature on QSS reveals several key limitations: an inability to support threshold reconstruction with fewer than all participants, insufficient privacy preservation regarding collaborator identities, lack of post-quantum authentication for participant verification, and absence of dynamic routing optimization for selecting the optimal subset of participants. These deficiencies collectively reduce the practical deployability of QSS in real-world distributed cloud systems.

This paper addresses these limitations by proposing a novel entanglement-based QSS framework. The principal contributions are: (i) a (t, n) -threshold QSS protocol that allows any t out of n players to reconstruct the secret; (ii) integration of a quantum-enhanced Dijkstra's algorithm with a custom weighting system for dynamic optimal participant selection; (iii) incorporation of CRYSTALS-Kyber post-quantum cryptographic primitives for robust player authentication and identity obfuscation; and (iv) a three-tier cloud-deployable system architecture enforcing centralized authorization, SHA-256 authenticated access control, and encrypted data storage.

The remainder of this paper is structured as follows: Section 2 reviews related work; Section 3 describes the proposed methodology; Section 4 presents the system architecture; Section 5 elaborates the implementation; Section 6 discusses results; and Section 7 concludes with future research directions.

2. LITERATURE SURVEY

Significant research has been conducted in quantum secret sharing, post-quantum cryptography, and quantum network optimization. Hillery, Bužk, and Berthiaume [8] first demonstrated QSS using GHZ tripartite entangled states, establishing the foundational model for quantum-secured secret distribution. Greenberger, Horne, and Zeilinger [9] further characterized multi-qubit entanglement properties essential for multi-party protocols. Liu et al. [7] introduced a QSS protocol with fairness guarantees, addressing the problem of participants receiving unequal advantages during secret reconstruction. Li, Chen, and Zhu [33] proposed a (t, n) -threshold scheme where only the dealer's interaction during the distribution phase is required, combining privacy features of secure multi-party computation with reusable secret shares.

Dynamic QSS protocols—which allow participants to join or leave without reissuing shares—were explored by Jia et al. [10], Liao et al. [11], Hsu et al. [12], and Mishra et al. [13]. Qin and Dai [14] extended dynamic QSS to d -dimensional GHZ states, while You et al. [15] demonstrated dynamic multiparty QSS using single photons. These works collectively highlight the importance of adaptive participant management in practical deployments.

Kang et al. [23] investigated continuous variable QSS with fairness, and Priyanka et al. [16] presented a (m, n) -threshold scheme employing quantum Fourier transforms with identity authentication. Tian et al. [22] demonstrated dynamic multiparty-to-multiparty QSS using Bell states, confirming scalability in complex topologies. Schauer, Huber, and Hiesmayr [25] proposed experimentally feasible security checks for n -qubit QSS providing verification methods adaptable to hardware implementations.

On the post-quantum cryptographic front, the CRYSTALS-Kyber key encapsulation mechanism, standardized by NIST, relies on the hardness of the Module Learning With Errors (MLWE) problem and provides strong resistance against quantum adversaries. Javadi-Abhari et al. [30] demonstrated the implementation feasibility of quantum circuits using IBM's Qiskit framework, validating simulation-to-hardware transfer of QSS-related protocols. Pan, Zhang, and Huang [31] addressed security bounds against Trojan-horse attacks in continuous-variable QKD systems, establishing passive optical countermeasures as critical security primitives.

Despite these advances, a unified framework that simultaneously addresses dynamic participant selection, post-quantum authentication, threshold reconstruction, and cloud integration remains absent from the literature. The proposed

protocol bridges this gap by combining quantum Dijkstra routing, CRYSTALS-Kyber authentication, and a (t, n) -threshold model within a deployable cloud architecture.

3. METHODOLOGY / PROPOSED SYSTEM

3.1 Problem Statement

Existing QSS protocols are constrained by static network topologies, the requirement for full shareholder participation (n -of- n schemes), the absence of post-quantum-secure authentication, and the lack of dynamic routing for optimal participant selection. These limitations prevent practical deployment in cloud environments where nodes are dynamic, infrastructure is heterogeneous, and adversaries may possess quantum computational capabilities.

3.2 Proposed Protocol Overview

The proposed framework constructs a QSS protocol over a generic distributed quantum network. The dealer distributes quantum-entangled shares to n players such that any t players ($t \leq n$) can collaboratively reconstruct the original secret, while any coalition of fewer than t players gains no information. This (t, n) -threshold property is achieved by exploiting quantum operators applied to entangled qubit registers, combined with symmetric polynomial-based secret encoding.

Player registration involves the submission of an email address and password, from which the system derives a unique network topology and assigns node weights encoding proximity to the dealer, fibre propagation properties, and link reliability metrics. The SHA-256 hash of the password serves as the authentication credential, ensuring that plaintext credentials are never stored or transmitted. Each player's data is subsequently encrypted using a CRYSTALS-Kyber public-private key pair generated during registration, providing IND-CCA2 security under the MLWE assumption.

3.3 Quantum Dijkstra Algorithm for Optimal Player Selection

A central innovation of the proposed system is the adaptation of Dijkstra's shortest-path algorithm into a quantum-weighted routing mechanism. The algorithm initializes a distance of zero at the source node (the dealer) and assigns infinity to all other nodes, iteratively selecting the unvisited node with the minimum tentative distance and relaxing all incident edges.

In the proposed quantum variant, edge weights are derived from entanglement fidelity estimates, fibre attenuation coefficients, and player-specific authentication scores. The algorithm dynamically computes the optimal subset of t players by selecting nodes whose cumulative quantum-weighted path cost is minimized. Players who fail authentication or whose channels exhibit high decoherence are automatically excluded, enhancing both security and reconstruction accuracy.

3.4 Security Framework

The protocol's security is analyzed against the extended CIA Triad, encompassing Confidentiality, Integrity, Availability, Authenticity, Accountability, and Non-repudiation. Confidentiality is maintained through Kyber-encrypted quantum shares; Integrity is enforced by SHA-256 authentication hashes; Availability is ensured by the threshold scheme permitting reconstruction with a subset of players; Authenticity is provided by Kyber key pair verification; Accountability is achieved via the Central Authority's download notification mechanism; and Non-repudiation is supported by cryptographically logged authorization events.

The protocol resists eavesdropping (quantum measurement disturbance detection), collusion attacks (players remain unaware of collaborator identities and network structure), Trojan-horse attacks (passive optical isolation at quantum interfaces), and identity spoofing (prevented by Kyber-authenticated key exchange).

4. SYSTEM ARCHITECTURE / DESIGN

4.1 Three-Tier Architecture

The system adopts a three-tier architecture comprising the Client Layer, the Processing Layer, and the Data/Security Layer. At the Client Layer, Players and Dealers interact through web-based interfaces. Players register with email and password, triggering automatic generation of a unique network topology with quantum weights; login is secured by SHA-256 hash verification. Dealers authenticate via user ID and password, gaining access to a dashboard for encrypted data retrieval and download request submission.

The Processing Layer is governed by the Central Authority (CA), which functions as the authorization and monitoring hub. The CA verifies dealer credentials prior to granting data access, authorizes all download requests, tracks data access events, and dispatches automatic notifications whenever a dealer retrieves data. The Data/Security Layer manages quantum-encrypted storage and network optimization operations. The Network Component maintains the weighted graph of player nodes, executing the quantum Dijkstra algorithm to select the optimal routing path for secret distribution and reconstruction.

4.2 Module Descriptions

The **Player Module** manages user registration, SHA-256 authentication, Kyber key pair generation, network topology visualization, and encrypted data storage. The **Dealer Module** handles dealer registration, authenticated login, encrypted data access, public key download, and authorized data requests. The **Central Authority Module** provides system-wide dealer authorization, activity logging, and download event notifications. The **Network Topology Module** implements the

quantum-weighted Dijkstra algorithm, maintaining the weighted graph of player nodes and computing optimal participant subsets for each secret-sharing session.

5. IMPLEMENTATION

5.1 Technology Stack

The backend is implemented in Java, leveraging Qiskit-compatible quantum simulation libraries for quantum circuit operations and entangled state preparation. Quantum circuit design and simulation are performed using IBM Quantum Experience and Qiskit, enabling validation of the QSS protocol on both simulated and real quantum hardware. The database layer employs a relational schema to store SHA-256 password hashes, Kyber public keys, and encrypted data blobs. The frontend provides browser-accessible registration, login, and data management interfaces for Players, Dealers, and the Central Authority.

5.2 Backend and Quantum Processing

The backend orchestrates secret encoding, quantum state simulation, and secure share distribution. Input data is converted into quantum state representations and processed through the QSS protocol pipeline using quantum entanglement-based encoding. The (t, n) -threshold share generation distributes encrypted quantum shares among registered players while maintaining the threshold reconstruction guarantee.

5.3 Quantum Protocol Execution

The QSS protocol execution begins with the dealer encoding the secret into a multi-qubit entangled state and distributing individual qubit shares to each of the n registered players. When reconstruction is initiated, at least t players submit their shares to the reconstruction oracle. The system verifies Kyber-authenticated identity for each contributing player, computes the quantum Dijkstra-optimized subset, and applies the inverse quantum operators to recover the original secret. Any attempt by fewer than t players to reconstruct yields no information, as guaranteed by the threshold property.

5.4 Cloud Integration and Access Control

Integration with cloud platforms such as Amazon Web Services or Microsoft Azure provides scalable storage for encrypted secret shares and enables multi-region distribution of player nodes. Access control policies enforce that only Kyber-authenticated, CA-authorized dealers may retrieve encrypted shares. All data transmissions occur over TLS-secured channels, providing an additional classical encryption layer atop the quantum security guarantees.

6. RESULTS AND DISCUSSION

The proposed QSS framework was evaluated through functional testing of the registration, authentication, secret sharing, and

reconstruction workflows, alongside security analysis against established threat models. The system successfully demonstrated end-to-end operation across all user roles: Players registering and generating network topologies, Dealers submitting authorized requests and retrieving encrypted data, and the Central Authority monitoring all data access events with real-time notifications.

The quantum Dijkstra algorithm correctly computed optimal player subsets across multiple simulated network configurations, demonstrating dynamic adaptability to varying node weights derived from entanglement fidelity and authentication scores. In all test scenarios with $t \leq n$ participants, threshold reconstruction was verified to succeed when exactly t or more Kyber-authenticated players submitted valid shares, while reconstruction attempts with fewer than t shares failed to recover any information—confirming the information-theoretic security property.

Fig. 1 illustrates the Home Page providing navigational access to all modules. Fig. 2 shows the Player Registration Page enabling secure account creation with topology generation. Fig. 3 depicts the Player Login Page enforcing SHA-256-based authentication. Fig. 4 and Fig. 5 show the Dealer Registration and Login interfaces with equivalent security controls. Fig. 6 presents the Central Authority Login Page restricting administrative access to authorized personnel.

CRYSTALS-Kyber authentication successfully prevented unauthorized access in all simulated impersonation attempts. SHA-256 password hashing ensured that no plaintext credentials were exposed at any system layer. The CA notification mechanism logged all dealer data access events, providing a complete audit trail for accountability enforcement. Compared to classical QSS protocols, the proposed system provides threshold reconstruction without full participant presence, resistance to quantum adversaries through Kyber encryption, dynamic participant selection via weighted quantum Dijkstra routing, and centralized accountability.

7. CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

This paper has presented a novel entanglement-based Quantum Secret Sharing protocol that simultaneously addresses threshold reconstruction, post-quantum authentication, dynamic participant selection, and cloud-deployable system architecture. The (t, n) -threshold scheme eliminates the need for full participant presence, while the quantum Dijkstra algorithm provides adaptive, performance-optimized routing. CRYSTALS-Kyber authentication ensures that only registered, verified players participate in reconstruction, substantially reducing identity spoofing and collusion risks. Security analysis confirms compliance with the extended CIA Triad, and simulation results

validate the protocol's correctness across multiple threshold configurations and network topologies.

7.2 Future Scope

Several avenues merit future investigation. While CRYSTALS-Kyber's security rests on the hardness of the MLWE problem, continued advances in quantum algorithms necessitate ongoing evaluation of post-quantum hardness assumptions. Future work should explore inherently quantum graph algorithms, such as quantum walk-based shortest-path methods, to further enhance participant selection efficiency.

Deployment on actual quantum hardware with error mitigation strategies, mid-circuit measurement capabilities, and quantum error-correcting codes represents a critical next step toward real-world operability. Extending the framework to support multi-level hierarchical secret sharing and incorporating privacy-preserving participant selection mechanisms would further strengthen the protocol's applicability. Integration with quantum repeater networks and satellite-based quantum communication links would enable geographically distributed deployments, fulfilling the vision of a globally interconnected quantum-secured cloud infrastructure.

REFERENCES

- [1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manage. Requirements Knowl.*, 1979, pp. 313–318, doi: 10.1109/AFIPS.1979.98.
- [2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979, doi: 10.1145/359168.359176.
- [3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.
- [4] C. Lu, F. Miao, J. Hou, W. Huang, and Y. Xiong, "A verifiable framework of entanglement-free quantum secret sharing with information-theoretical security," *Quantum Inf. Process.*, vol. 19, no. 1, 2020, Art. no. 24, doi: 10.1007/s11128-019-2509-x.
- [5] B. C. Hiesmayr, "Free versus bound entanglement, a NP-hard problem tackled by machine learning," *Sci. Rep.*, vol. 11, no. 1, 2021, Art. no. 19739, doi: 10.1038/s41598-021-98523-6.
- [6] R. van Houten et al., "Mathematical formulation of quantum circuit design problems in networks of quantum computers," *Quantum Inf. Process.*, vol. 19, no. 5, 2020, Art. no. 141, doi: 10.1007/s11128-020-02630-8.
- [7] F. Liu, S.-J. Qin, and Q.-Y. Wen, "A quantum secret-sharing protocol with fairness," *Phys. Scripta*, vol. 89, no. 7, 2014, Art. no. 075104, doi: 10.1088/0031-8949/89/7/075104.
- [8] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, pp. 1829–1834, 1999, doi: 10.1103/PhysRevA.59.1829.
- [9] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," 2007, arXiv:0712.0921.

- [10] H.-Y. Jia et al., "Dynamic quantum secret sharing," *Phys. Lett. A*, vol. 376, nos. 10–11, pp. 1035–1041, 2012.
- [11] C.-H. Liao, C.-W. Yang, and T. Hwang, "Dynamic quantum secret sharing protocol based on GHZ state," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1907–1916, 2014, doi: 10.1007/s11128-014-0779-x.
- [12] J. L. Hsu, S. K. Chong, T. Hwang, and C. W. Tsai, "Dynamic quantum secret sharing," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 331–344, 2013.
- [13] S. Mishra et al., "An integrated hierarchical dynamic quantum secret sharing protocol," *Int. J. Theor. Phys.*, vol. 54, no. 9, pp. 3143–3154, 2015.
- [14] H. Qin and Y. Dai, "Dynamic quantum secret sharing by using d-dimensional GHZ state," *Quantum Inf. Process.*, vol. 16, no. 3, 2017, Art. no. 64.
- [15] Z. You et al., "Dynamic quantum secret sharing between multiparty and multiparty based on single photons," *Phys. A*, vol. 624, 2023, Art. no. 128893.
- [16] P. Priyanka, V. Siwach, and P. Bijarianian, "Quantum secret sharing with (m, n) threshold: QFT and identity authentication," *Quantum Inf. Process.*, vol. 23, 2024, Art. no. 348.
- [17] N. Zhou et al., "Multi-party semi-quantum private comparison protocol of size relation with d-level GHZ states," *Adv. Quantum Technol.*, 2024, doi: 10.1002/qute.202400530.
- [18] L. Gong et al., "Novel semi-quantum private comparison protocol with Bell states," *Laser Phys. Lett.*, vol. 21, no. 5, 2024, Art. no. 055209.
- [19] W. Hu et al., "A novel dynamic quantum secret sharing in high-dimensional quantum system," *Quantum Inf. Process.*, vol. 20, no. 5, 2021, Art. no. 159.
- [20] Y. Song, Z. Li, and Y. Li, "A dynamic multiparty quantum direct secret sharing based on generalized GHZ states," *Quantum Inf. Process.*, vol. 17, no. 9, 2018, Art. no. 244.
- [21] C.-W. Yang and C.-W. Tsai, "Improved dynamic multiparty quantum direct secret sharing protocol based on generalized GHZ states to prevent collusion attack," *Modern Phys. Lett. A*, vol. 35, no. 8, 2020, Art. no. 2050040.
- [22] Y. Tian et al., "Dynamic multiparty to multi-party quantum secret sharing based on Bell states," *Adv. Quantum Technol.*, vol. 7, no. 7, 2024, Art. no. 2400116.
- [23] Y. Kang et al., "Continuous variable quantum secret sharing with fairness," *Appl. Sci.*, vol. 10, no. 1, 2020, Art. no. 189.
- [24] X. Li et al., "A new quantum multiparty simultaneous identity authentication protocol with the classical third-party," *Entropy*, vol. 24, no. 4, 2022, Art. no. 483.
- [25] S. Schauer, M. Huber, and B. C. Hiesmayr, "Experimentally feasible security check for n-qubit quantum secret sharing," *Phys. Rev. A*, vol. 82, no. 6, 2010, Art. no. 062311.
- [26] G. Gao, C.-C. Wei, and D. Wang, "Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states," *Quantum Inf. Process.*, vol. 18, no. 6, 2019, Art. no. 186.
- [27] R. Golden and I. Cho, "On symmetric polynomials," 2015, arXiv:1511.08870.
- [28] K. Thas, "The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs," *Europhys. Lett.*, vol. 86, no. 6, 2009, Art. no. 60005.
- [29] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.
- [30] A. Javadi-Abhari et al., "Quantum computing with Qiskit," 2024, arXiv:2405.08810.
- [31] Y. Pan, L. Zhang, and D. Huang, "Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution," *Phys. Rev. Appl.*, vol. 21, 2024.
- [32] Z. Ji, P. Fan, and H. Zhang, "Entanglement swapping theory and beyond," *Phys. Rev. Lett.*, vol. 132, 2024.
- [33] F. Li, T. Chen, and S. Zhu, "A (t,n) threshold quantum secret sharing scheme with fairness," *Quantum Inf. Process.*, vol. 22, 2023.