AQSC: A Multi-Stage Quantum Protocol Chain

Combining QKD, QDL, and QSDC over Quantum Networks

Ali Nasser
University of Babylon, Iraq
alinasser.sec@student.uobabylon.edu.iq
https://a360n.github.io

Submitted: June 15, 2025

An interactive version of this paper is available at:
https://a360n.github.io/aqsc-project/

Abstract

Ali Quantum Secure Chain (AQSC) is a proposed layered framework that integrates three fundamental quantum communication protocols—Quantum Key Distribution (QKD), Quantum Data Locking (QDL), and Quantum Secure Direct Communication (QSDC)—into a unified security chain operating over a quantum networking infrastructure.

The framework aims to provide full-spectrum quantum security: QKD ensures the generation of secret keys with physical-level security; QDL enables efficient quantum data encryption using extremely small classical keys; and QSDC allows the direct and secure transmission of messages via quantum channels.

By combining these protocols in a sequential and interoperable architecture, AQSC offers both immediate and forward-looking solutions for secure communication in the quantum era. This paper outlines the motivation, structure, and potential applications of AQSC, forming a foundation for future development, open-source simulation, and real-world deployment.

1. Introduction

The advent of quantum computing poses a significant threat to classical cryptographic systems, particularly those based on asymmetric key algorithms such as RSA and ECC. As quantum algorithms like Shor's and Grover's continue to evolve, the urgency to develop quantum-resilient communication protocols becomes more critical.

In response to this challenge, the field of quantum communication has produced several powerful but distinct protocols. Quantum Key Distribution (QKD) enables two parties to establish a shared secret key with security guaranteed by the laws of quantum mechanics. Quantum Data Locking (QDL) allows large quantum information to be locked using surprisingly small classical keys, offering efficient quantum encryption. Quantum Secure Direct Communication (QSDC), in contrast, allows messages to be transmitted directly over quantum channels, eliminating the need for key distribution altogether.

Although each of these protocols offers a unique contribution to the field of quantum security, they are often studied and implemented in isolation. There remains a critical gap in the literature and practice: a unified framework that combines these protocols in a structured, interoperable manner to maximize communication security at every layer.

In this paper, we introduce the Ali Quantum Secure Chain (AQSC - a multistage quantum communication model that integrates QKD, QDL, and QSDC over a quantum networking infrastructure. AQSC is designed to operate as a security chain, where each stage builds upon the previous, enabling a full-spectrum defense against classical and quantum-level threats.

The following sections describe each protocol involved, explain how AQSC chains them together, and discuss potential real-world applications where such an integrated model is not only beneficial, but essential.

2. Background

2.1. Quantum Key Distribution (QKD)

Quantum Key Distribution is one of the most mature and widely studied quantum communication protocols. It allows two parties (commonly called Alice and Bob) to establish a shared secret key, with security rooted in the no-cloning theorem and the disturbance caused by measurement. Notable protocols include BB84 and E91, which leverage photon polarization or entanglement to detect any eavesdropping attempt. The final output is a classical key that is used in subsequent encryption systems.

2.2. Quantum Data Locking (QDL)

Quantum data lock is a lesser-known but powerful concept in quantum cryptography. It enables a large amount of quantum information to be locked using a surprisingly small classical key. Without the key, the data appears indistinguishable from noise. QDL leverages the fundamental limits of quantum measurements, where the amount of retrievable information is restricted unless the correct basis or unitary operation is known. This makes QDL especially useful in scenarios where secure quantum data storage or transfer is needed.

In the context of AQSC, the data being locked through QDL is assumed to be *quantum-native*—i.e., inherently quantum information rather than classical data encoded into quantum states. This design decision enables seamless integration with QSDC, which directly transmits quantum states while preserving their integrity and confidentiality. However, AQSC can also support classical-to-quantum encoding in alternative configurations where QDL is applied to classical information represented in quantum form.

2.3. Quantum Secure Direct Communication (QSDC)

QSDC is a protocol for sending actual message content directly over quantum channels — without the need for prior key distribution. It combines quantum entanglement and secure transmission protocols to ensure message integrity and immediate eavesdropping detection. Unlike QKD, QSDC does not produce a key; instead, it transmits the message itself with quantum-level protection.

2.4. Quantum Networking

Quantum Networking refers to the physical and logical infrastructure that enables the exchange of quantum information across distributed nodes. It includes quantum channels (e.g., optical fiber or free-space links), quantum repeaters, entanglement distribution, and synchronization mechanisms. Quantum networks are essential for scalable implementation of QKD, QSDC, and future quantum internet applications. AQSC is designed to operate entirely over such infrastructure, treating it as a foundation layer.

3. The AQSC Framework

The Ali Quantum Secure Chain (AQSC) is a layered communication framework designed to provide end-to-end quantum security by integrating three core quantum protocols—QKD, QDL, and QSDC—into a sequential, interoperable chain operating over a quantum network.

Each stage of AQSC is responsible for a specific layer of security:

Stage 1: Quantum Key Distribution (QKD)

The communication process begins with QKD to establish a shared, quantum-secure classical key between Alice and Bob. This key will later serve as the basis for encrypting quantum data in the next stage. QKD also serves as the first line of defense, detecting any potential eavesdropping on the channel.

Stage 2: Quantum Data Locking (QDL)

Once a key has been successfully distributed, Alice uses it to "lock" the quantum data she wishes to transmit. This process applies a series of quantum operations (e.g., rotations, permutations) that render the data unreadable without the key. The strength of QDL lies in its ability to use extremely short keys to protect large quantum states.

Stage 3: Quantum Secure Direct Communication (QSDC)

The locked quantum data is then transmitted directly to Bob via a quantum channel using QSDC. QSDC ensures that the transmission itself is inherently secure and actively monitors for any intrusion or tampering. If an attack is detected, the transmission can be aborted, and the chain reset.

Protocol Integration Rationale

While QKD and QSDC are often treated as distinct or even competing protocols—one relying on prior key distribution and the other transmitting information directly without a key—AQSC employs them in a complementary sequence. In this framework, QSDC is not used as a standalone encryption protocol, but rather as a secure quantum transport layer for transmitting QDL-locked quantum data.

By first using QKD to establish a classical secret key, we enable QDL to lock sensitive quantum information using minimal key material. QSDC then serves as a highly secure delivery mechanism, ensuring that the transmission of this locked data remains tamper-evident and resistant to interception. This design leverages the strengths of each protocol to construct a layered and redundant security chain.

Protocol Flow

AQSC follows a strict linear structure:

- QKD generates a secret key.
- QDL locks data using the key.
- QSDC delivers the locked data to the receiver.

This layered design ensures that even if a vulnerability exists in one stage, the other layers continue to protect the communication integrity and confidentiality.

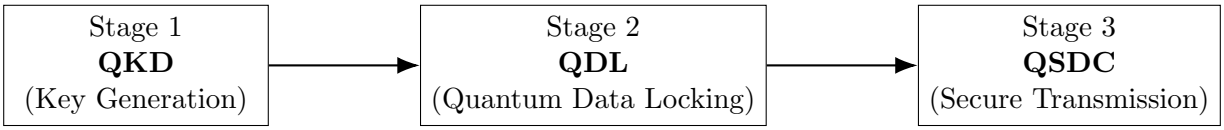

Figure 1: AQSC Protocol Flow: From Quantum Key Generation to Secure Direct Communication

Implementation Assumptions

- All communication occurs over a functioning quantum network capable of supporting entanglement distribution and QKD channels.
- The parties (Alice and Bob) are equipped with quantum transmitters and receivers.

- Quantum memories are not strictly required for all AQSC operations. However, certain implementations of QDL may benefit from short-term quantum memory, particularly for buffering, synchronization, or intermediate state storage during complex locking operations.

Comparison with Isolated Protocols

While QKD, QDL, and QSDC are powerful individually, each has limitations when deployed alone. By chaining them, AQSC:

- Achieves both key-based and direct message security.
- Provides redundant layers of eavesdropping detection.
- Offers quantum-level encryption with minimal key size overhead.
- Enables adaptability to various communication scenarios: real-time, offline, or hybrid.

4. Benefits and Use Cases

Key Benefits

The AQSC framework offers several advantages over using individual quantum communication protocols in isolation:

- Full-spectrum security: By chaining QKD, QDL, and QSDC, AQSC secures every layer—from key generation to message transmission—ensuring end-to-end confidentiality and integrity.
- Built-in redundancy: If one layer is compromised or attacked, the others continue to protect the communication. For instance, even if an attacker manages to intercept the quantum channel during QSDC, they cannot read the data without the QDL key.
- Eavesdropping detection: Both QKD and QSDC incorporate native mechanisms for detecting interference. This makes AQSC highly resistant to man-in-the-middle and interception attacks.
- Minimal key size: QDL allows locking large amounts of quantum data using short classical keys, improving efficiency without sacrificing security.
- Scalability: The framework is designed to operate over quantum networks, allowing for future adaptation to large-scale, multi-node environments.

Use Cases

- **Government and Military:**

  AQSC can be deployed in national defense communication systems, enabling secure command transmission even over long-distance or satellite-based quantum networks. Its layered protection makes it ideal for scenarios requiring both real-time and covert transmission.

- **Quantum Cloud Computing:**

  With the growing interest in blind quantum computing and secure cloud-based quantum processing, AQSC provides a foundation for transmitting encrypted quantum jobs and retrieving results without exposing sensitive data.

- **Healthcare and Genomic Data:**

  Medical institutions can use AQSC to protect genomic data or medical imaging transmitted between facilities, preserving both privacy and regulatory compliance (e.g., HIPAA or GDPR in quantum contexts).

- **Financial Networks:**

  Banks and fintech platforms can utilize AQSC to secure high-value transaction channels where traditional cryptography may be vulnerable to future quantum attacks.

- **Critical Infrastructure:**

  Utilities and infrastructure operators can integrate AQSC into control systems (e.g., smart grid, transportation, space systems) where system integrity and availability are mission-critical.

Potential Deployment Models

- Point-to-point model for direct communication between two secure facilities.
- Star topology with a centralized secure node distributing keys and coordinating communication.
- Mesh network integration in future quantum internet infrastructure for resilient, decentralized communication.

5. Limitations and Challenges

While AQSC presents a promising layered approach to quantum communication security, several technical and practical challenges must be acknowledged:

- **Protocol synchronization:** Coordinating the timing between QKD, QDL, and QSDC stages requires precise synchronization mechanisms. Any drift or delay may result in data misalignment or loss.
- **Quantum memory and buffering:** Although AQSC minimizes the reliance on long-term quantum memory, certain use cases—especially involving QDL—may benefit from short-term quantum storage for buffering or retransmission.
- **Noise sensitivity in QSDC:** QSDC channels are inherently sensitive to noise and quantum decoherence. Maintaining fidelity over long distances remains a significant engineering challenge.
- **Scalability and infrastructure:** The implementation of AQSC assumes access to a robust quantum networking infrastructure, which may not yet be available or scalable in many real-world environments.
- **Standardization and interoperability:** Each protocol in AQSC may be implemented differently across vendors or research platforms. Ensuring interoperability across stages remains a non-trivial task.

These limitations highlight the need for further research, simulation, and experimental validation of AQSC in realistic settings before large-scale deployment becomes feasible.

6. Conclusion and Next Steps

This paper has presented AQSC—Ali Quantum Secure Chain—as a multi-stage quantum communication framework that sequentially integrates QKD, QDL, and QSDC into a unified, layered architecture. Designed to operate over quantum networking infrastructure, AQSC aims to deliver full-spectrum security by leveraging the combined strengths of each protocol.

By addressing both theoretical vulnerabilities and real-world deployment challenges, AQSC offers a resilient and adaptable solution for quantum-era communication. It ensures end-to-end confidentiality, efficient quantum encryption, eavesdropping detection, and readiness for future integration into quantum internet architectures.

Next Steps

This brief paper serves as the conceptual foundation for the following planned phases:

- Open-source tool development: A lightweight simulation of the AQSC framework will be developed using Python and Qiskit, and published as an open-source GitHub repository.
- Interactive web portal: A publicly accessible website will present a visual summary of the paper, conceptual diagrams, and links to key resources.
- Full research paper: A comprehensive follow-up paper will include detailed simulations, performance analysis, and expanded use cases.
- Global infrastructure vision: A long-term proposal will outline how AQSC could be deployed in real-world quantum networks as part of a scalable, secure communication infrastructure.

The AQSC initiative represents a new direction in quantum communication—one that emphasizes integration, interoperability, and robust security across every stage of quantum information transfer.

References

1. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, 1984.
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.
3. S. Lloyd, "Quantum Enigma Machines," *Science*, vol. 321, pp. 1463–1465, 2008.
4. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, 2012.
5. G. Long and X. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, 2002.
6. Q. Zhang et al., "Quantum Secure Direct Communication with Quantum Memory," *Nature Communications*, vol. 8, 2017.

7. H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, 2008.

8. S. Muralidharan et al., "Optimal architectures for long distance quantum communication," *Scientific Reports*, vol. 6, 2016.

9. C. H. Bennett et al., "Quantum information theory," *Physics Today*, vol. 48, no. 10, pp. 24–30, 1995.

10. S. Pirandola et al., "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

11. C. H. Bennett and P. W. Shor, "Quantum Information Theory," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2724–2742, 1998.

12. F. Xu, X. Ma, Q. Zhang, et al., "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics*, vol. 92, 025002, 2020.

13. J.-Y. Guan, et al., "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 9, no. 1, 2020.

14. M. Lucamarini, Z. L. Yuan, et al., "Overcoming the rate–distance limit of quantum key distribution," *Nature*, vol. 557, pp. 400–403, 2018.

15. R. Van Meter and S. J. Devitt, "The path to scalable distributed quantum computing," *Computer*, vol. 49, no. 9, pp. 31–42, 2016.

16. S. Pirandola et al., "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, pp. 397–402, 2015.

17. L. Gyongyosi and S. Imre, "A Survey on Quantum Computing Technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

18. F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block," *Physical Review A*, vol. 68, 042317, 2003.

19. R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, pp. 865–942, 2009.

20. S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, eaam9288, 2018.