Quantum Secure Messaging Protocol (QSMP)

Revision: 3.0
Date: October 10, 2025
Author: John G. Underhill
Document Type: Executive Summary
Keywords: QSMP, Quantum-Secure Messaging, SIMPLEX, DUPLEX, RCS, Kyber, McEliece, Dilithium, SPHINCS+, Post-Quantum AEAD

1. Overview

The **Quantum Secure Messaging Protocol (QSMP)** is a high-assurance, post-quantum secure transport protocol that defines two interoperable operational modes: **SIMPLEX** (one-way trust, client-server) and **DUPLEX** (mutual trust, peer-to-peer). It provides authenticated, encrypted, and integrity-checked channels resistant to all known quantum and classical attacks.

QSMP's design philosophy rejects legacy protocol layering and negotiation complexity. Instead, it establishes cryptographic certainty through deterministic configuration, explicit authentication, and authenticated packet framing. It is engineered to serve as a **core secure transport primitive** across the QRCS protocol stack, enabling future systems to operate securely in environments where traditional public-key infrastructures will fail under quantum attack.

By using lattice or code-based post-quantum primitives with a Rijndael-derived authenticated stream cipher (**RCS**), QSMP achieves both cryptographic durability and operational speed. Its unified handshake model allows adaptive deployment from embedded systems to enterprise networks without modification.

2. Motivation and Strategic Rationale

Modern infrastructures rely on encryption schemes; RSA, ECC, ECDH, that will be rendered vulnerable by large-scale quantum computing. Many institutions recognize this, but few possess architectures designed from inception for the post-quantum transition. QSMP fills that void.

Where existing secure channels (TLS, SSH, IPSec) depend on layer-negotiated or versioned cipher-suites, QSMP's mechanism is **non-negotiable** and **parameter-bound**, ensuring consistent cryptographic posture across deployments. This prevents downgrade attacks and simplifies certification and compliance.

Strategically, QSMP represents a **foundational investment in future-proof communications**. It mitigates "harvest-now, decrypt-later" risk by providing resistance at both data-in-transit and key-management layers. The dual-mode SIMPLEX/DUPLEX architecture allows QRCS and its licensees to span markets from consumer IoT to critical infrastructure without fragmenting protocol design, reducing development cost and accelerating time-to-adoption.

For acquirers and strategic partners, QSMP forms a defensible, standards-aligned intellectual property asset: it is patent-pending, modular, portable across platforms, and directly addresses the 2025-2035 post-quantum migration market.

3. Architecture and Mechanism

QSMP employs two cryptographic handshakes, each optimized for a specific trust topology:

SIMPLEX Mode - One-Way Trust (Client-Server):

The client validates the server's signature and encapsulation key, performs a **KEM-based encapsulation,** and derives symmetric session keys via SHAKE and KMAC functions. The resulting 256-bit transmit and receive keys initialize an RCS cipher instance providing authenticated encryption with associated data (AEAD). SIMPLEX achieves full session establishment in two round-trips, minimizing latency and resource overhead, ideal for high-volume or stateless endpoints.

DUPLEX Mode — Mutual Trust (Peer-to-Peer):

Both participants exchange signed encapsulation keys, producing two independent shared secrets that are combined through a cryptographic key-derivation function into distinct transmit and receive keys. This dual-contribution scheme guarantees explicit key confirmation and bilateral authenticity, eliminating the possibility of unilateral key manipulation. DUPLEX is suited for high-assurance systems where both parties require verified trust, such as inter-agency or cross-domain networks.

Across both modes, QSMP's framing structure is deterministic and compact. Each packet header embeds a **flag, sequence number, payload length, and UTC time window**, all included in AEAD authentication to enforce replay resistance and temporal validity. Session state is minimal, and cryptographic material is ephemeral, ensuring forward secrecy and compartmentalization.

The protocol supports **Kyber** or **McEliece** for key encapsulation, **Dilithium** or **SPHINCS+** for signatures, **SHA-3/SHAKE** for hashing and key derivation, and the **RCS authenticated stream**

cipher for data confidentiality and authentication. These components collectively define a balanced cryptographic stack resistant to both classical and quantum adversaries.

4. Security Model and Post-Quantum Posture

QSMP's security model aligns with the Authenticated and Confidential Channel Establishment (ACCE) framework. It guarantees the following:

- **Authentication:** SIMPLEX ensures authenticated servers; DUPLEX ensures mutual authentication.
- **Confidentiality:** All data packets are encrypted under session-unique keys derived from IND-CCA-secure KEM secrets.
- **Integrity:** RCS AEAD enforces block-wide authentication with no unverified plaintext leakage.
- **Forward Secrecy:** Ephemeral KEM keypairs are destroyed immediately after session derivation.
- **Replay Resistance:** Each packet is bound to a UTC timestamp and sequence counter authenticated under AEAD.
- **Post-Compromise Security:** Optional ratcheting refreshes symmetric keys through one-time KDF derivations.

QSMP intentionally omits negotiable parameters to prevent downgrade or reflection attacks. The security assumptions rest on the quantum hardness of underlying primitives and the non-malleability of AEAD authentication. Protocol teardown occurs upon any verification failure, ensuring zero recovery bias or oracle surface.

Cryptographically, QSMP's construction positions it as a **quantum-resilient successor** to TLS and SSH, providing higher assurance with less complexity and stronger isolation of session contexts.

5. Implementation and Integration

QSMP's reference implementation is written to MISRA-C standards, ensuring deterministic and auditable execution across Windows, macOS, and Linux environments. The codebase provides portable headers and simple C APIs for initialization, handshake, and AEAD operations.

Integrators can link QSMP as a **secure transport layer** beneath existing protocols or as a direct replacement for TLS in embedded or constrained systems. SIMPLEX is optimized for servers managing tens of thousands of clients, maintaining minimal per-session memory (<4 KB). DUPLEX integrates seamlessly with long-lived peer-links where periodic rekeying is enforced by topology.

The protocol's stateless framing enables embedding within UDP, QUIC, or custom transports, while its deterministic message structure eases formal verification. Internally, its modular cryptographic primitives (RCS, SHA-3, KMAC, PQ KEMs) align with the broader QRCS ecosystem.

6. Use Cases and Applications

QSMP's dual-mode design allows deployment across multiple verticals:

Critical Infrastructure and Defense:
DUPLEX mode provides peer-authenticated, dual-key tunnels between command systems and distributed nodes with non-repudiable message integrity.

Financial Networks:
SIMPLEX delivers high-speed, low-latency secure connections for trading systems, fintech platforms, and blockchain gateways requiring constant session turnover.

Enterprise Cloud and Zero-Trust Architectures:
As a post-quantum alternative to TLS or IPSec, QSMP provides forward-secure VPN and service-mesh overlays with deterministic policy enforcement.

IoT and Industrial Systems:
SIMPLEX's minimal footprint and two-RTT handshake make it ideal for constrained devices, secure telemetry, and remote-control environments.

Government and Diplomatic Communications:
DUPLEX mode's explicit key confirmation and bilateral trust are suited for cross-border or classified data exchange.

Collectively, these applications illustrate QSMP's flexibility as a unified transport foundation spanning from edge to core infrastructure.

7. Economic and Operational Value

From an operational standpoint, QSMP offers measurable efficiency. Its constant-time cryptography, lightweight session memory, and CPU-accelerated RCS cipher yield high concurrency and low latency per session. These efficiencies translate directly into reduced infrastructure cost, fewer cryptographic dependencies, and lower integration overhead compared to multi-layered TLS stacks.

For acquirers and strategic investors, QSMP represents **defensible intellectual property:**

- Proprietary handshake models (SIMPLEX/DUPLEX) and packet framing.
- Original RCS authenticated cipher architecture.
- MISRA-compliant reference implementation proven across three major OS platforms.
- Clear forward integration with existing QRCS protocol families.

These elements form a strong portfolio component for organizations seeking leadership in post-quantum secure communications and exportable cryptographic technology.

8. Long-Term Security Benefit

QSMP reinforces a future where **privacy and integrity are sustainable beyond quantum transition.** By standardizing deterministic, authenticated communication patterns, it provides a foundation for global systems, financial, governmental, scientific, to operate securely under evolving computational paradigms.

Its open architecture and interoperability with NIST PQC standards promote responsible adoption without vendor lock-in. As part of the QRCS ecosystem, QSMP contributes to an industry shift toward provably durable communications that respect both sovereignty and data integrity across borders.

9. Conclusion

The Quantum Secure Messaging Protocol exemplifies the QRCS design philosophy: **clarity, certainty, and cryptographic permanence**. Through its dual-mode SIMPLEX and DUPLEX structure, authenticated AEAD transport, and strict post-quantum construction, QSMP delivers a defensible, scalable, and standards-aligned secure messaging solution.

For acquirers, it represents a cornerstone technology with clear pathways into next-generation VPNs, distributed control systems, financial infrastructure, and national defense communications. It is a mature, well-engineered protocol positioned not as an incremental evolution of legacy secure channels, but as their quantum-resistant successor — a foundation for the secure Internet of the post-quantum era.

Prepared by: Quantum-Resistant Cryptographic Solutions
Contact: contact@qrcscorp.ca