QSMP

The Quantum Secure Messaging Protocol

A quantum ready, high-security messaging protocol for a new age

QSMP

The Quantum Secure Messaging Protocol

QSMP: Security for a New Age

The twenty-first century has brought a new era of discovery and rapidly advancing technological capabilities. Quantum computers, once thought impossible to build, are now becoming a reality. Along with the development of machine intelligence, these technologies promise to accelerate our technological evolution at an unprecedented rate. Billions of dollars are being invested in these emerging industries, and the achievement of strong AI—machines capable of human-like reasoning and deduction—is expected within this century. While these advancements in science and technology hold great potential if used wisely, they also pose serious threats to the security of communication systems that underpin all aspects of human commerce and communication.

Despite the urgency of these changes, many in industry and government continue to underestimate the scope and scale of the impact that quantum computing will have on existing security systems. The challenges of scaling quantum computers have largely shifted from theoretical obstacles to engineering problems, which are steadily being solved. Meanwhile, AI research is progressing towards true machine intelligence. Yet, the adaptation to this evolving threat is slow, and we are not prepared for what is coming.

Cryptography is often viewed through an economic lens, seen more as a commodity than a critical security measure. Large corporations dominate standardization bodies, focusing on reducing costs rather than ensuring long-term security. This has led to the widespread adoption of cryptographic primitives that lack the robustness needed to face future challenges. Strong cryptography does exist, but it is frequently dismissed as being too costly for the web industry. As a result, outdated protocols and weak parameter sets have become the norm, setting the stage for future vulnerabilities in the world's security infrastructure.

QSMP Overview

QSMP is a set of encrypted tunneling protocols designed using state-of-the-art post-quantum secure ciphers and cryptographic protocols. It offers a versatile toolset that can replace aging protocols like TLS and SSH. The QSMP protocol includes two tunneling implementations: **Duplex** and **Simplex**.

- **Duplex Protocol**: In the Duplex implementation, a two-way trust is established between hosts, with each party possessing the other's public signature verification key. Both hosts generate asymmetric cipher key pairs, exchange public keys and ciphertexts, and authenticate all parts of the bi-directional exchange using asymmetric signature schemes. The two shared

secrets derived from this exchange create 512-bit symmetric session keys that initialize RCS-512, a Rijndael-based authenticated symmetric stream cipher. Duplex is designed as a client-to-client encrypted tunnel, delivering maximum security between connected hosts.

- **Simplex Protocol**: The Simplex implementation relies on one-way trust, where the client verifies the server's asymmetric public cipher key and ciphertext using a public signature verification key distributed to clients. Simplex uses a single shared secret to derive session keys that initialize the RCS-256 authenticated symmetric stream cipher. This high-performance, multi-threaded server implementation can handle hundreds of thousands of simultaneous connections.

Applications of QSMP

QSMP is a flexible platform suitable for various applications, including remote access tunnels, secure trading systems, communication channels, or any implementation requiring a post-quantum secure encrypted tunnel. Its generic design allows it to operate as a self-contained encrypted tunnel, making data accessed through the tunnel invisible to the application layer and accessible with only a few simple function calls.

Supported Cryptographic Primitives

QSMP supports several cryptographic primitives that are finalists in the NIST Post-Quantum Cryptography competition:

- **Asymmetric Ciphers**: McEliece, Kyber
- **Asymmetric Signature Schemes**: Dilithium, SPHINCS+
- **Symmetric Cryptography**: RCS, an authenticated stream cipher based on the wide-block Rijndael (AES) cipher, strengthened with a hash-based key expansion function and additional transformation rounds.

Long-Term Security

We prioritize long-term security over cost-efficiency, aiming to provide a flexible security paradigm that offers realistic long-term protection against future threats. QSMP uses RCS, a symmetric stream cipher designed to address vulnerabilities in AES, specifically related to its key schedule. RCS incorporates a cryptographically-strong key expansion function and is seen as the future of the Rijndael family of symmetric ciphers.

Robust Authentication

QSMP emphasizes advanced authentication techniques, using both quantum-resistant asymmetric and symmetric primitives. The protocol employs post-quantum signature schemes for key exchange authentication, with packet authentication secured by the NIST SHA-3 KMAC function.

Versatility in Deployment

QSMP's versatility allows it to be used in many configurations: as a secure messaging platform, a component in financial systems, personal messaging clients, remote control of machines, or as the backbone of a commodity trading system. QSMP is the premier choice for applications requiring high-security, quantum strength, and true long-term resilience.

Commitment to Excellence

Our focus is not on the cheapest solutions but on the most secure ones. We aim to place long-term security back at the forefront of cryptographic development. QSMP is not burdened with trade-offs that sacrifice security for performance; instead, it stands as the most secure cryptographic messaging protocol available today, designed to meet the needs of a rapidly evolving technological landscape.