Ambit Client CNSA 2.0 Compliant Post-Quantum VPN with MaxKyber Protocol by American Binary

Version 2.0.0 | June 2026

Abstract

Ambit Client enterprise VPN combines fully Commercial National Security Algorithm Suite 2.0 (CNSA 2.0[1]) compliant post-quantum cryptography (PQC) with networking performance improvements to mitigate both the cryptographic security impacts of quantum computing and the operational friction commonly induced by post-quantum cryptographic security products. Underlying these capabilities is an innovative network protocol, *MaxKyber*[2], that enables rapid, modular replacement of classical cryptographic protocols anticipated to be vulnerable to quantum computers with secure PQC algorithms within a framework that replaces legacy tunneling protocols such as IPSec and WireGuard. Featuring a formally third party-verified cryptographic foundation fully compliant with CNSA 2.0 National Security System requirements, high-performance networking stack, and enterprise architecture support make it suitable for protecting not only mission-critical cybersecurity infrastructure but commercial enterprises' remote workers, on-premises networks, cloud deployments, and more against both current and future adversaries, including nation-states.

Editor's Note: In no way shape or form are we claiming that NSA has endorsed this technology. MaxKyber has been validated by exhaustive third-party peer-reviewed as fully complying with NSA's CNSA 2.0 requirements.

11335 NE 122nd Way, Suite 105
Kirkland, WA 98034
Contact: sales@ambit.inc

Table of Contents

1 Executive Summary

"While organizations today are increasingly recognizing the significance of PQC, American Binary has been preparing for a post-quantum world for seven years. The result is a resilient foundation for secure operations, today and in the post-quantum future" - Oracle

Ambit Client enterprise VPN combines fully Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) compliant post-quantum cryptography (PQC) with networking performance improvements to mitigate both the cryptographic security impacts of quantum computing and the operational friction commonly induced by post-quantum cryptographic security products.

Underlying these capabilities is an innovative network protocol, *MaxKyber*, that enables rapid, modular replacement of classical cryptographic protocols anticipated to be vulnerable to quantum computers with secure PQC algorithms within a framework that replaces legacy tunneling protocols such as IPSec and WireGuard.

Featuring a formally third party-verified cryptographic foundation fully compliant with Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) National Security System requirements, high-performance networking stack, and enterprise architecture support make it suitable for protecting not only mission-critical cybersecurity infrastructure but commercial enterprises' remote workers, on-premises networks, cloud deployments, and more against both current and future adversaries, including nation-states.

Key features include:

- Full compliance with CNSA 2.0 National Security System requirements for networking
- Uniquely low overhead, with ~4,600 less bytes per handshake packet when compared to the most common CNSA 2.0 implementations, ensuring performance in low-bandwidth and degraded network conditions
- Crypto-agility: ad hoc replacement of cryptographic algorithms via

- Nanosecond-level latency in high-performance deployments using Vector Packet Processing / Data Plane Development Kit, validated on Oracle Cloud Infrastructure at 15 Gbps throughput (line rate) with support for 1Tbps throughput and beyond
- Protocol formally verified using both Tamarin and ProVerif, with 120 security properties proven covering key exchange, authentication, forward secrecy, denial-of-service protection, resource exhaustion, and implementation correctness
    - Expert cryptographic review by Dr. Tom Shrimpton, PhD
    - Formal specification review by Dr. Joe Kiniry, PhD
- FPGA hardware acceleration implementation has been developed on Xilinx platforms, with all cryptographic operations executing on FPGA fabric – the CPU never touches session keys or plaintext
- ESP32-S3 support
- TCP fallback transport implemented and security-analyzed for environments where UDP is blocked
- MTU-aware packet segmentation protocol with adaptive Forward Error Correction (FEC) implemented and formally specified
- Enterprise zero trust features as defined by zero trust requirements for National Security Systems on track to be implemented by end of 2026
- Support for Windows, Mac, iOS, Android, and Linux (Ubuntu, RedHat, etc.) across the following architecture categories:
    - Point to Point (Basic, Redundant)
    - Hub & Spoke (Single, Active/Active, Active/Standby, Hierarchical)
    - Mesh (Full, Partial)
    - Access (Remote, DMZ Gateway, Extranet/B2B)
    - Cloud (Site-to-Cloud, Multi, Hybrid)
    - Datacenter (Interconnect, Geo-Redundant, HA Cluster)
    - Segmentation (Single, Multi-Tenant, IoT/OT)

These features ensure the reliability, resilience, efficiency, and maintainability of *Ambit Client VPN* as a foundation for modern cybersecurity operations – from protecting orchestration workflows and sensor telemetry to enabling secure threat intelligence sharing across organizational boundaries.

2 Introduction

Quantum computing poses an existential threat to the cryptography that secures the modern connected ecosystem. Adversarial cryptographically relevant quantum computers (CRQC) are expected by 2030. Mitigation of this threat requires a synergy of three elements: New cryptography that is resistant to quantum attack, the availability of products that use the new cryptography, and versatile, modular implementations of the new cryptography that accelerate the proliferation of the post-quantum product ecosystem.

Confidence in the quantum emergence timeline is such that state and non-state actors have invested heavily in the capture and storage of all traffic traversing the Internet. These actors do so based on a set of well-founded assumptions:

- While they are currently unable to exploit data captured due to the pervasive use of classical asymmetric cryptography, CRQC will enable them to decrypt the data;
- A significant portion of the information contained in the captured data has long-term value[3]; and
- Once decrypted, they will be able to exploit the information to their benefit

This activity is known as a Harvest-Now-Decrypt-Later (HNDL) attack[4], and is ongoing on a broad, prolific, and pervasive scale at the time of this paper's writing. HNDL obsoletes current cryptographic algorithms and security and privacy mechanisms such as virtual private networks (VPN).

Industry, academia, and government have not been idle with respect to the quantum threat. A new class of cryptography, designed expressly to be quantum resilient, has emerged. Collectively, these algorithms are referred to as PQC. Three PQC algorithms were standardized in August 2024 by the United States National Institute of Standards and Technology (NIST) [5].

In 2022, the U.S. government issued the Commercial National Security Algorithm Suite, version 2.0 (CNSA 2.0), specifically identifying six cryptographic algorithms as sufficient for providing post-quantum cryptographic resistance. These include ML-KEM (FIPS 203) for key establishment, ML-DSA (FIPS 204) for digital signatures, AES with 256-bit keys, SHA with 384- or 512-bit outputs, the Leighton-Micali Signature (LMS) scheme, and the Extended Merkle Signature Scheme. A clarifying FAQ (December 2024, Version 2.1) stated

in pertinent part: *RSA and Elliptic Curve Cryptography are the main algorithms that need to be replaced to achieve quantum resistance*. Additionally, the Diffie-Hellman key exchange is not considered quantum-resistant according to CNSA 2.0 and therefore all its variations must be replaced.

U.S. government policy establishes that all network equipment (including VPNs) must support and prefer CNSA 2.0 PQC as the default in 2026, all new National Security System acquisitions must be CNSA 2.0 compliant by January 1, 2027, and all legacy products are required to fully transition to CNSA 2.0 PQC by December 31, 2031.

While PQC standardization is unequivocally positive, the nature of the algorithms presents challenges to broad implementation and adoption. These range from network performance degradation to inconsistencies with common systems' interconnection protocols and the dearth of mature security protocols providing expected capabilities, such as in-session key rotation.

This paper provides insight into a new class of VPNs, typified by American Binary's *Ambit Client VPN* product, doing so through the lens of American Binary's modular post-quantum network protocol, *MaxKyber*. The paper provides a detailed description of the *MaxKyber* key establishment process, its formal verification evidence, and the enterprise platform's suitability for protecting modern cybersecurity infrastructure.

3 Ambit Client VPN

VPNs are popular and prolific for good reasons. By using encryption, a VPN creates a secure connection over a less secure or insecure network such as the public Internet. VPNs make use of tunneling protocols[6] to establish a secure connection between clients and servers. A VPN supports and secures common use cases such as remote and distributed workforces, Internet Protocol (IP) address management, bypassing throttling controls, and the safe use of publicly available internet connections.

Success, for a modern VPN, is defined as supporting four requirements:

- **Security:** The VPN protects data and sensitive information against potential breaches or leaks, whether at the hands of insider or external threats, and whether inadvertent or malicious in nature. Security is achieved when a person's or organization's private information and data cannot be accessed or modified by

unauthorized actors and when authorized users have assured access to the information and data.

- **Privacy:** The VPN renders users' connections and activity opaque to eavesdroppers between the users' devices and the VPN server, ensuring that users can conduct operations without unauthorized interference or intrusion. Privacy is achieved when users are able to exert control over how personal information and data are collected, stored, and used. Consequently, security can exist without privacy, but security is a pre-requisite for privacy.
- **Performance:** Security technology has an unfortunate and often deserved reputation for creating bottlenecks and degradations in operational and network performance. To provide the greatest benefit, a VPN product must provide the expected security and privacy guarantees with as little performance impact as possible. Ideally, the VPN's networking architecture either complements that of the network medium over which it operates or obviates the network medium's native bottlenecks and other latency-inducing mechanisms to improve performance.
- **Quantum resilience:** VPNs rely on cryptography to deliver their security and privacy guarantees. It is anticipated that quantum computing will obsolete the classical cryptography used for providing information confidentiality and integrity as well as the exchange and establishment of cryptographic key material. To be effective in both the current pre-quantum (i.e., HNDL attack) and post-quantum eras, a VPN must exclusively implement standardized PQC algorithms and avoid using the Diffie-Hellman key exchange.[7]

In response to the market need emerging from these requirements, American Binary developed the *Ambit Client VPN*. *Ambit Client VPN* provides robust security guarantees for operations in both the pre- and post-quantum eras through the exclusive use of PQC that is strictly consistent with CNSA 2.0 requirements.[8] To meet the performance requirements implicit for a modern VPN, *Ambit Client VPN* makes use of a fast, innovative networking technology called Vector Packet Processing (VPP)[9] with Data Plane Development Kit (DPDK) kernel-bypass acceleration, and optionally, FPGA hardware acceleration of all cryptographic operations.

3.1 Ambit Client VPN Architectural Overview

Figure 1 portrays the *Ambit Client VPN* functional architecture:

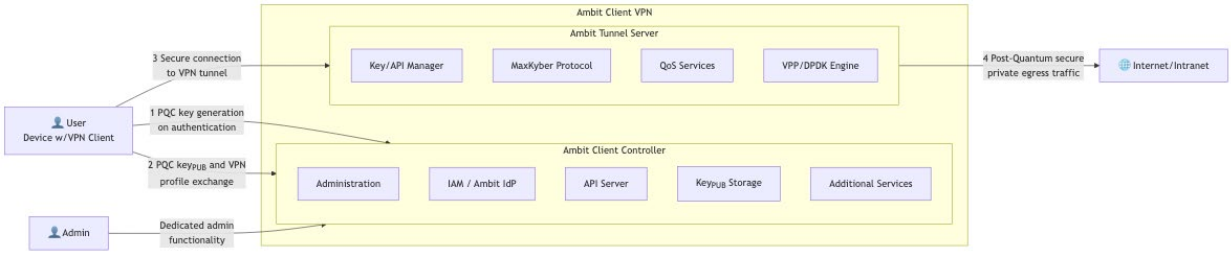

Figure 1, Ambit Client VPN Architectural Overview

Ambit Client VPN comprises three primary components:

- A **client application** that runs on endpoint devices including Microsoft Windows and Apple macOS desktops and Android and Apple iOS mobile devices;
- A **controller server** (*Ambit Client Controller* or ACC) configurable to support delivery as either a Software-as-a-Service (SaaS) or on-premises product; and
- A **tunnel server** (*Ambit Tunnel Server* or ATS) configurable to support delivery as either a SaaS or on-premises product

The client application is user-facing and enables users to connect their endpoints to (and disconnect from) the VPN.

The ACC comprises five major subcomponents: an administration module, an identity and access management (IAM) capability via Ambit Client Identity Provider integration (supporting OAuth 2.0/OIDC), an application programming interface (API) server, storage for peers' public keys, and a set of various administrative services that ensure robust, high-quality service. Collectively, the ACC provides the VPN's administrative and management framework with multi-tenant organization support and role-based access control (System Owners, Customer Administrators, Users).

The ATS comprises three major subcomponents: a combined key and API manager, the *MaxKyber* protocol engine, and a set of various quality-of-service (QoS) services. Collectively, the ATS provides secure tunnel connections from authorized endpoints to the ATS, and, when so configured, from the ATS to other ATSs within a mesh or point-to-point (P2P) network. The ATS integrates with VPP/DPDK for user-space packet processing, achieving line rate throughput with microsecond-level latency, and optionally with FPGA hardware acceleration for environments requiring the highest cryptographic performance.

3.2 Ambit Client VPN Operational Sequence

A typical *Ambit Client VPN* sequence of operations when operating as a SaaS is described below.

Step	Operational Event
0	*Ambit Client VPN* contains a suite of administration tools that support its use within an enterprise context. These include discrete tool sets and control surfaces for **System Owners**, who are responsible for managing the overall system as well as customer accounts and financial operations, and **Customer Administrators**, who are responsible for managing their specific customer account or accounts. This functionality is logically distinct from VPN operations but is essential for the operation of the delivered product
1	As part of installation on an endpoint device, the client application generates an ML-KEM-1024 keypair (FIPS 203). **The private key never leaves the device**. The client application enables the user to initiate a connection to the VPN
2	Upon connection initiation, the ML-KEM public key and the parameters for the interaction between the client and the tunnel server, referred to as the VPN profile, are created. The ACC validates the device, verifies group-based authorization, and provisions the public key to the selected tunnel server
3	Once the VPN profile is established, it is used within the context of the *MaxKyber* protocol to securely establish symmetric keys[10] governing the encrypted session between the client and the tunnel server. Once the keys are established, a secure VPN session between the client and the tunnel server is initiated
4	Once the VPN session is initiated, the client can reach the Internet or organizational intranet in a private and secure manner. All traffic is encrypted with AES-256-GCM using session keys derived from post-quantum key exchange

3.3 Zero Trust Architecture

The *Ambit Client VPN* platform is being designed for alignment with prevailing zero trust architectural frameworks by end of 2026. Key zero trust principles to be implemented include:

- **Never Trust, Always Verify**: Every connection attempt is authenticated through ML-KEM key exchange. No implicit trust based on network location or other factors
- **Least Privilege Access**: Device and user authorization decisions are made per-connection through the peer group controller with group-based access policies
- **Assume Breach**: The *MaxKyber* protocol's defense-in-depth design (signature-free KEM handshake, optional PSK, forward secrecy) ensures that compromise of any single component does not result in complete security failure
- **Continuous Verification**: Automatic key rotation with configurable intervals ensures continuous cryptographic freshness. Session keys rotate approximately every hour or after 2^60 messages
- **Device Identity**: ML-KEM keypairs generated on-device during onboarding bind cryptographic identity to specific endpoints
- **Micro-segmentation**: Peer group controller enables fine-grained network segmentation through routing and ACL policies with multi-tenant isolation

The core of *Ambit Client VPN* is the *MaxKyber* protocol that supports post-quantum encrypted networking.

4 MaxKyber Cryptographic Protocol

The *MaxKyber* protocol was designed to meet a number of technical challenges impacting PQC implementation, including:

- Making the new PQC algorithms functionally useful by packaging them in a modular manner such that they could be readily integrated into any product requiring the secure exchange of information across a potentially insecure channel. This includes VPNs, such as *Ambit Client VPN*, and also networking and connectivity tools like software defined networks (SDN), browsers, and cloud services
- Ensuring that common features such as in-session key rotation were provided in a manner consistent with PQC cryptographic standards and CNSA 2.0. For example,

the ML-KEM standard is silent on the issue of key rotation[11], which is a standard part of legacy cryptographic protocols like Internet Key Exchange, v.2 (IKEv2)

- Ensuring the provision of a robust, post-quantum **analog** to the key establishment capabilities provided by classical cryptographic protocols such as the elliptical curve Diffie-Hellman key agreement protocol (ECDH) that was faithful to PQC standards and the requirements specified in CNSA 2.0
- Ensuring compatibility with existing networking standards and implementations. For example, PQC algorithms often run into issues with Maximum Transmission Unit (MTU) limitations.[12] This constraint becomes of singular importance when mobile and Internet-of-Things (IoT) networks are considered
- Solving the key distribution problem between peers in a manner consistent with CNSA 2.0 without exposing a shared secret (e.g., a cryptographic key) to the risks of transit across an insecure channel

The *MaxKyber* protocol is implemented as a modular package that is portable to a wide range of products, thus offering a short path to rapid, prolific PQC adoption. It is defined in a comprehensive RFC-like engineering specification document (Revision 24, March 2026, 90+ pages) that has undergone expert cryptographic review by Dr. Tom Shrimpton, PhD and formal specification review by Dr. Joe Kiniry, PhD.

4.1 MaxKyber Cryptographic Primitives

MaxKyber uses the following CNSA 2.0-aligned cryptographic primitives:

Primitive	Algorithm	Standard	Security Level
Key Encapsulation	ML-KEM-1024	FIPS 203	NIST Level 5
Symmetric Encryption	AES-256-GCM	FIPS 197	256-bit (128-bit post-quantum)
Hash Function	SHA-512/256	FIPS 180-4	256-bit
MAC	HMAC-SHA512/256	FIPS 198-1	PRF-secure
Key Derivation	HKDF-SHA512/256	RFC 5869	Based on HMAC

ML-KEM-1024 is based on the Module Learning With Errors (M-LWE) problem, a lattice-based problem that is mathematically verified to be secure against both classical and quantum adversaries. ML-KEM-1024 provides NIST Level 5 security – even with quantum computers, breaking 128-bit security requires 2^128 quantum operations, which is infeasible. The "1024" refers to the security parameter; actual keys are 1568 bytes for public keys and 3168 bytes for secret keys.

4.2 MaxKyber Architectural Overview

Figure 2 portrays the *MaxKyber* functional architecture:

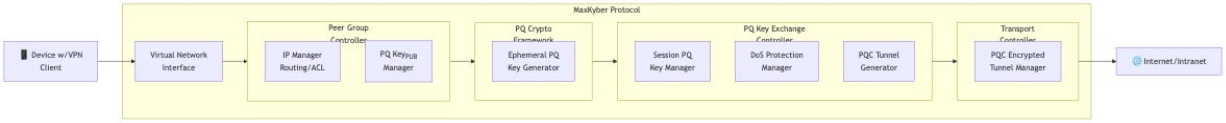

Figure 2, MaxKyber Functional Architecture

The *MaxKyber* protocol comprises five primary components:

- A **virtual network interface** governing connections from clients seeking to access the protocol's services;
- A **peer group controller** that manages public keys belonging to known peers and provides network control services including IP management and routing/ACL policies;
- A **post-quantum cryptographic framework** that generates post-quantum public keys and assists with key derivation using HKDF-SHA512/256;
- A **post-quantum key exchange controller** that manages session keys, provides denial-of-service (DoS) attack protection via a cookie mechanism, and generates the post-quantum cryptographic tunnels between clients and the tunnel server; and
- A **transport controller** supporting UDP (primary) and TCP (fallback) that manages tunnels in use with automatic key rotation and keepalive management

4.3 MaxKyber Signature-Free KEM Handshake

The core innovation of *MaxKyber* is its signature-free KEM handshake architecture. Classical protocols such as TLS 1.3 and IKEv2 rely on digital signatures (RSA, ECDSA) for authentication during key exchange. *MaxKyber* eliminates signatures entirely, achieving mutual authentication exclusively through key encapsulation operations. This is significant

because it removes an entire class of cryptographic primitive from the protocol's attack surface while maintaining all required security properties.

The fundamental challenge in transitioning from Diffie-Hellman to a KEM-based key exchange is asymmetry. Diffie-Hellman allows both parties to independently derive the same shared secret through the commutativity property. KEMs are inherently one-directional – the encapsulator generates a random shared secret and encrypts it to the decapsulator's public key. *MaxKyber* addresses this through a carefully designed multi-stage KEM handshake adapted from the Noise protocol framework that achieves the following properties without any signature operations:

- **Mutual authentication**: Both initiator and responder cryptographically prove their identity through successful KEM decapsulation. An adversary possessing only public keys cannot impersonate either party
- **Identity hiding**: The initiator's identity is protected from passive observers. Even if an adversary intercepts the handshake, they cannot determine who initiated the connection without the responder's private key
- **Perfect forward secrecy**: Ephemeral keys are generated per-session and erased after use. Compromise of long-term static keys cannot retroactively expose past session traffic
- **Post-compromise security**: Regular rekeying (~1 hour intervals) ensures that even temporary key compromise does not provide long-term access
- **Key Compromise Impersonation (KCI) resistance**: Compromising one party's static key does not enable an adversary to impersonate the *other* party. This property has been formally verified in Tamarin

An **optional** pre-shared key (PSK) can provide defense-in-depth. The protocol achieves full CNSA 2.0 post-quantum security without PSK; PSK adds a symmetric security layer that remains effective even if ML-KEM is later found vulnerable to a novel mathematical attack.

4.4 MaxKyber Protocol Operational Sequence

The sequence diagram in Figure 3 illustrates the *MaxKyber* protocol operational sequence. The handshake establishes a secure tunnel in a single round trip (1-RTT):

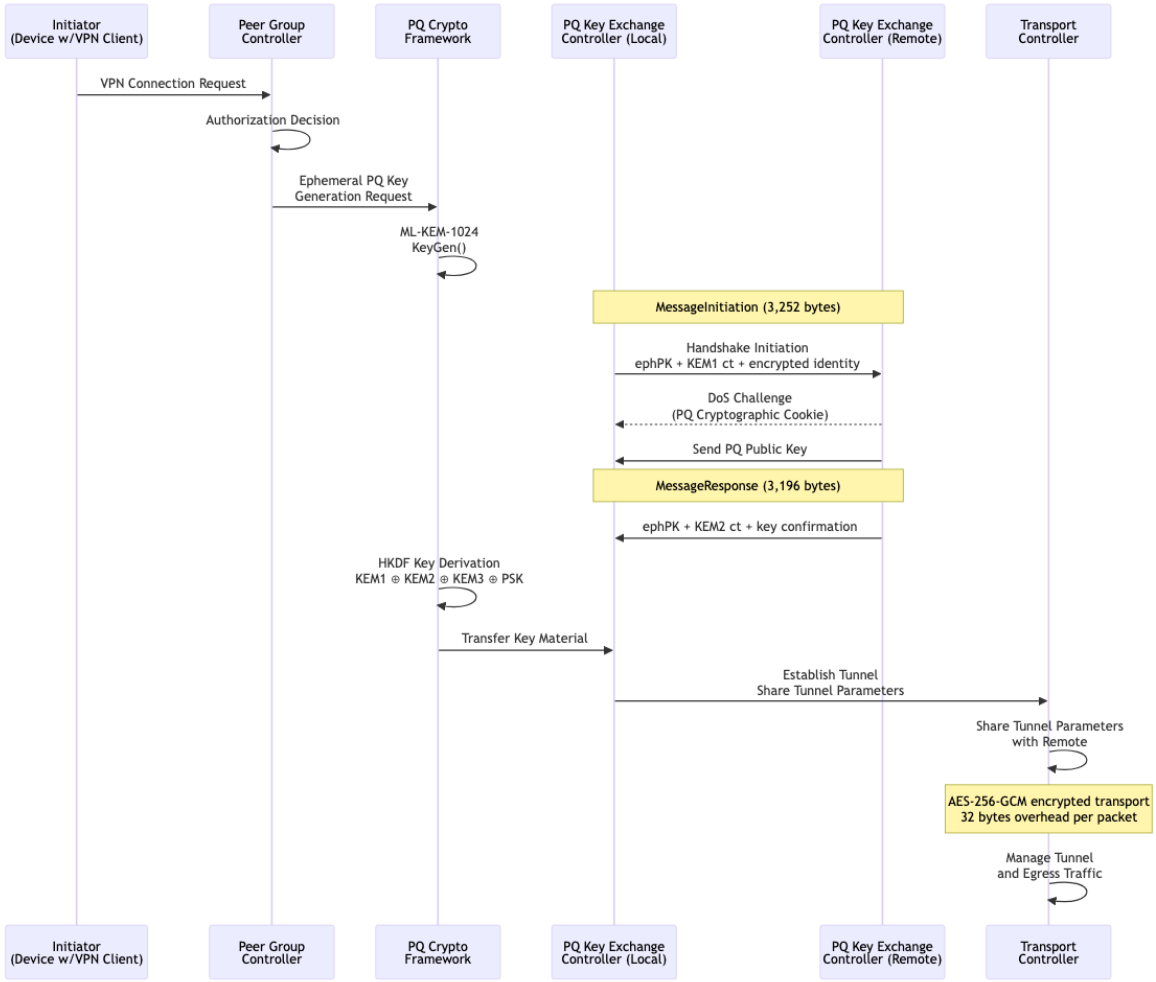

Figure 3, MaxKyber Operational Sequence

4.5 Packet Segmentation and Forward Error Correction

Post-quantum handshake messages (~3.2KB) exceed typical MTU sizes (1,500 bytes), necessitating a segmentation layer. *MaxKyber* includes a formally specified segmentation protocol – the Universal Multipath Transformer – that:

- Fragments handshake messages into MTU-compliant segments with 36-byte headers containing 128-bit cryptographic SessionIDs
- Provides reliable, ordered reassembly with timeout management
- Includes DoS protection through rate limiting (per-source: 300 slots, 200 segments/second) and bounded resource allocation (global: 10,000 simultaneous reassemblies)

- Supports networks ranging from jumbo frames (9,000 bytes) to IPv6 minimum (1,280 bytes)
- Enables **multipath reassembly**: segments can arrive from different network paths (WiFi, cellular, satellite simultaneously), reassembled using (SessionID, SegmentID) tuples
- Includes **adaptive Forward Error Correction** (FEC) using Reed-Solomon codes:

The Initiator Exception Rule – a novel, patent-pending solution to the FEC bootstrapping paradox – allows initiators to enable FEC after 3 failed attempts without creating amplification vulnerability, since the initiator already knows the server exists and cannot be used as an amplification target.

FEC Level	Data Segments	Parity Segments	Success at 50% Loss
None	3	0	12.5%
Light	3	1	31.2%
Medium	3	3	65.6%
Heavy	3	6	91.0%
Extreme	3	9	98.0%

4.6 TCP Fallback Transport

For environments where UDP is blocked or unreliable (affecting approximately 3% of users, primarily behind WiFi extenders dropping UDP), *MaxKyber* provides a TCP fallback transport:

- Wraps standard *MaxKyber* protocol messages in a TCP stream with magic header validation (“MKTCP002”)
- Server listens for incoming TCP connections; clients behind NAT connect outbound
- Maintains all cryptographic security properties of the UDP transport
- Rate-limited (30 connections/minute recommended) with 5-second connection timeouts
- Used for handshakes only; data transport remains UDP for performance

4.7 Mobile and Enterprise Features

- **Simultaneous Handshake Handling**: Explicit state machine logic handles simultaneous handshake attempts from both peers, critical for mobile networks where connectivity restoration causes both peers to timeout and retry simultaneously. Formally verified in Tamarin
- **Sleep/Wake Detection**: Detects device power state transitions (activity gaps >45 seconds) and adjusts retry timing with progressive backoff (10s, 15s, 30s, 60s, 3min), informed by MOBIKE (RFC 4555) reactive detection philosophy
- **Endpoint Migration**: Supports dynamic IP address changes (WiFi to cellular handoff) with replay-window binding to prevent replay-to-migrate attacks. Anti-replay nonces tracked per-keypair
- **Silent Operation**: Peers do not respond to unauthenticated packets, making port scanning ineffective. Passive observers cannot determine if a UDP port is running *MaxKyber*

5 Formal Verification

"No known VPN—post-quantum or classical, deployed or research — has been subjected to specification and formal verification of comparable depth" -Dr. Joe Kiniry, PhD and Dr. Tom Shrimpton, PhD

The *MaxKyber* protocol's security properties have been formally verified using a dual-tool approach achieving complete coverage across 120 security properties and 395 traceability elements. This verification effort represents a significant advance beyond the security assurances available for most deployed cryptographic protocols.

5.1 ProVerif

ProVerif uses Horn clause resolution to verify non-injective security properties, completing all queries in approximately 24 hours:

Category	Properties Verified

Core key exchange	Session key secrecy under quantum adversary
Authentication	Non-injective authentication in both directions
Privacy	Initiator identity hiding from passive observers
DoS protection	Cookie mechanism correctness and resource bounds
State machine	Correct state transitions under all message orderings
Segmentation	Fragment reassembly correctness and security
Cryptographic primitives	Correct usage of ML-KEM, AES-GCM, HKDF
PSK properties	Defense-in-depth under ML-KEM compromise
Key lifecycle	Rekeying maintains security properties

5.2 Tamarin

Tamarin uses constraint-based backward search to verify injective properties with explicit trace semantics. A novel **hierarchical decomposition technique** was developed to overcome a source saturation problem specific to multi-stage KEM protocols – standard Tamarin analysis cycles indefinitely due to cyclic dependencies in such protocols. The technique exploits the causal ordering of protocol events to decompose verification into independent phases. Results include but are not limited to:

- **Injective Correspondence**: Proves each successful session maps to exactly one matching initiation
- **KCI Resistance**: Compromising one party's key cannot impersonate the other party
- **Edge-Case Models**: Error handling, ignored responses, simultaneous initiation, traffic padding – all verified in under 1 second

5.3 Verified Security Property Categories

The 120 security properties fall into the following 11 categories:

Property	Verified By	Description

Session Key Secrecy	Both	Session keys remain secret from quantum adversaries
Transport Data Secrecy	Both	Transport data remains secret from quantum adversaries
Forward Secrecy	Both	Past sessions secure even if current keys compromised
Mutual Authentication	Both	Both peers prove identity via KEM decapsulation
Message Authentication	Both	All messages are authenticated
Identity Hiding	ProVerif	Initiator identity protected from passive observers
Replay Protection	Both	Anti-replay nonces prevent replay-to-migrate attacks
DoS Resistance	ProVerif	Cookie mechanism prevents resource exhaustion
KCI Resistance	Tamarin	Compromising one party's key cannot impersonate other
Resource Exhaustion	ProVerif	Critical resources are protected from artificial exhaustion
Key Agreement	Both	Key agreement unilaterally enforced

5.4 Expert Cryptographic Review

The protocol underwent review by Tom Shrimpton (82 individual annotations) and Joe Kiniry (13 formal specification annotations). All substantive concerns from the cryptographic review were addressed in RFC Revisions 21-24, including resolution of the computational bound contradiction in the threat model, comprehensive error handling specification (fail-closed behavior), exact MAC coverage with byte offsets, corrected authentication timing claims, and rekeying synchronization documentation.

Overall, ~12,000 lines of specification were created across 24 documents and ~5,900 lines of formal models across 16 files used across 9 Tamarin models and 7 ProVerif models.

5.5 Advisory Validation

American Binary's approach to post-quantum cryptography and protocol design has been supported by advisors Whitfield Diffie and Bruce Schneier. Brian LaMacchia has conducted a deep review of the underlying technology. Their involvement reflects a commitment to ensuring that the *MaxKyber* protocol and the *Ambit Client VPN* platform meet the highest standards of cryptographic rigor.

6 High-Performance Networking

6.1 VPP/DPDK Integration

The *Ambit Tunnel Server* integrates with Vector Packet Processing (VPP) and Data Plane Development Kit (DPDK) for wire-speed performance:

- **User-Space Networking**: Bypasses kernel network stack via DPDK poll-mode drivers for microsecond-level packet processing
- **memif Shared Memory**: Zero-copy packet transfer between *MaxKyber* protocol engine and VPP forwarding graph
- **Batch Processing**: VPP processes packets in vectors for improved cache locality, achieving 1-2 million packets per second
- **Validated Deployment**: Tested on Oracle Cloud Infrastructure with VPP 25.10 and DPDK 25.07.0, achieving 15 Gbps throughput (line rate) with support for 1Tbps throughput and beyond

6.2 FPGA Hardware Acceleration

For the highest performance requirements, American Binary has developed FPGA implementations targeting Xilinx platforms:

- **All crypto on FPGA fabric**: AES-256-GCM, SHA-512/256, SHA-3/Keccak, ML-KEM-1024 NTT, HKDF, and hardware TRNG (SP 800-90A/B) – the CPU never touches session keys or plaintext
- **Thousands of concurrent peers** in on-chip memory with microsecond-level context switching
- **Constant-time execution**: No secret-dependent branching; one-hot byte decode; no dividers

- **Open-source design**: 31 cryptographic modules, zero black boxes, zero vendor-encrypted IP

7 Securing Cybersecurity Infrastructure

The threat landscape facing modern organizations demands that cybersecurity infrastructure itself be protected with the same rigor applied to the data it defends. Cybersecurity sensors, orchestration platforms, and intelligence sharing systems are high-value targets – compromising them provides adversaries with visibility into defensive posture, the ability to blind defenders, and lateral movement pathways through privileged access.

Existing cybersecurity infrastructure typically relies on TLS 1.2/1.3 with ECDH, IPSec VPNs with RSA or ECDH, and API authentication via RSA-signed tokens – all of which are vulnerable to a CRQC. The *Ambit Client* platform replaces this vulnerable foundation with exclusively CNSA 2.0-compliant post-quantum cryptography across all communications paths.

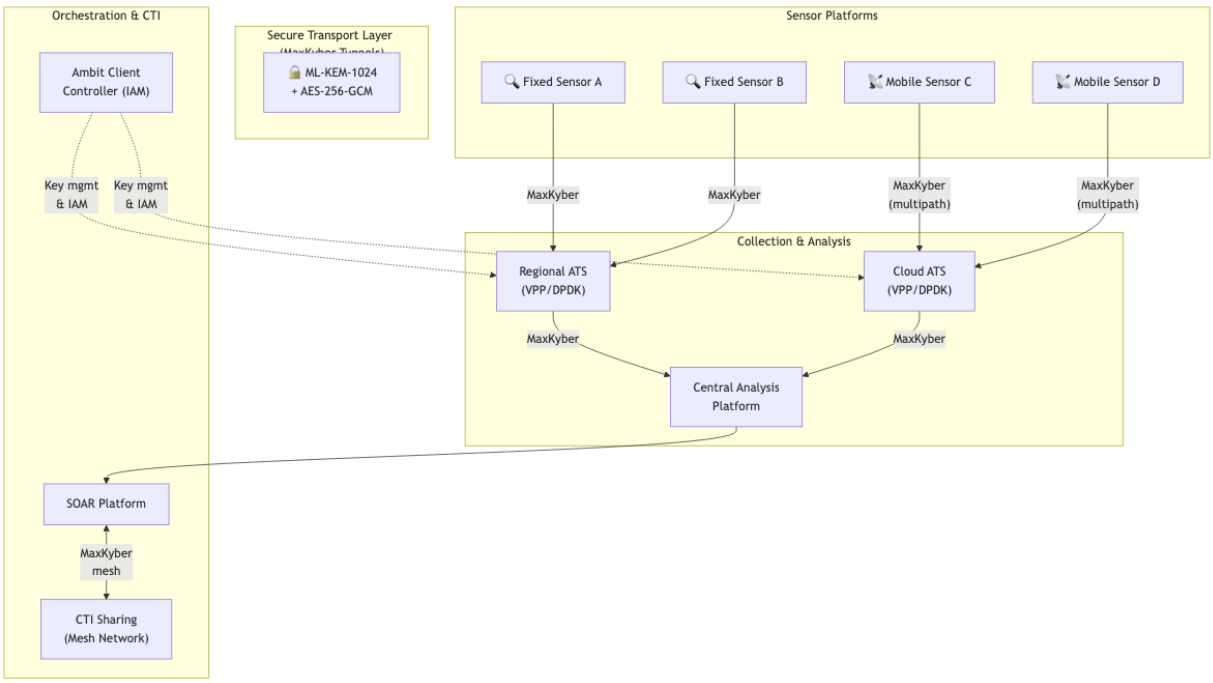

Figure 4, Sensor and Orchestration Architecture

7.1 Orchestration Services

Cybersecurity orchestration platforms – SOAR systems, configuration management tools, automated response systems – require both a secure control plane (commands, policies, playbook updates) and a secure data plane (alert data, log streams, telemetry). *Ambit Client VPN* protects both:

- **Post-quantum encrypted control plane**: All orchestration commands carried over *MaxKyber* tunnels with ML-KEM-1024 authenticated key exchange, AES-256-GCM encryption, and forward secrecy via ephemeral KEM
- **Zero trust orchestration access**: Per-node ML-KEM identity with no shared credentials, least-privilege peer group policies, and automatic key rotation ensuring compromised credentials expire
- **Multi-domain isolation**: Separate *MaxKyber* tunnels per security domain with independent key material through the ACC's multi-tenant organization management
- **Complete workflow protection**: From alert ingestion through analysis, response decision, action execution, and feedback – each link secured by mutually authenticated, encrypted channels

7.2 Cyber Threat Intelligence Sharing

Effective cybersecurity requires sharing threat intelligence across organizational boundaries. *MaxKyber*'s properties are well-suited for this:

- **Identity hiding**: The initiator's identity is encrypted during the handshake, protecting the identity of CTI sources from passive observers (formally verified in ProVerif)
- **Mesh networking**: The ATS supports peer-to-peer, hub-and-spoke, hierarchical, and redundant mesh topologies for CTI distribution
- **Traffic analysis resistance**: Silent operation, 16-byte payload padding, indistinguishable keepalives, and uniform handshake sizes resist adversary fingerprinting of sharing activity
- **Access control**: Multi-tenant architecture maps to CTI partnerships with independent cryptographic isolation; partner revocation is immediate via public key removal

7.3 Sensor Platform Modernization

Cybersecurity sensor platforms require modernized connectivity addressing post-quantum security, high bandwidth, low latency, mobility, and scalability. *Ambit Client VPN* provides:

- **On-sensor key generation**: ML-KEM keypairs generated on the sensor device bind cryptographic identity to specific hardware; private keys never leave the device
- **High-performance transport**: VPP/DPDK acceleration supports high-bandwidth sensor data streams; FPGA offload for the highest throughput requirements
- **Mobile sensor support**: Endpoint migration for dynamic IP environments, sleep/wake detection for battery-powered platforms, simultaneous handshake handling for reconnection, and multipath reassembly across WiFi + cellular
- **Scalable fleet management**: Automated onboarding, centralized key rotation, profile distribution, and group-based authorization through the ACC API
- **Flexible architectures**: Hub-and-spoke, regional aggregation, mesh sensor networks, and hybrid topologies – all with *MaxKyber* tunnels on every link

8 Summary of MaxKyber vs Classical Cryptography (ECDH)

Feature	**Classical Cryptography (ECDH)**	MaxKyber **(Post-Quantum)**
Security Basis	Elliptic Curve Discrete Logarithm Problem (ECDLP)	Lattice Learning with Errors (M-LWE)
Quantum Resistance	Vulnerable to quantum attacks (Shor's algorithm)	Resistant to quantum attacks (NIST Level 5)
Key Exchange Process	4x Diffie-Hellman (symmetric commutativity)	Signature-free ML-KEM-1024 handshake
Handshake Size	~240 bytes	~6,448 bytes (with segmentation)
Per-Packet Overhead	32 bytes	32 bytes

Authentication	Static key DH operations	Signature-free KEM mutual authentication (formally verified)
Forward Secrecy	Via ephemeral DH	Via ephemeral KEM (keys erased after use)
Formal Verification	Limited Tamarin model	Tamarin + ProVerif dual verification (85+ properties)
DoS Protection	Cookie mechanism	Cookie mechanism (equivalent) with rate limiting
Segmentation	Not needed (small messages)	Built-in MTU-aware with multipath and FEC
CNSA 2.0 Compliance	Non-compliant	Fully compliant
Hardware Acceleration	Software only	FPGA with all crypto on fabric

9 Summary

Ambit Client VPN is the first of a new generation of VPN products that combine fully CNSA 2.0 compliant PQC (without any classical cryptography) with networking improvements to both mitigate the impacts of quantum computing on the connected environment's cryptographic foundations and the operational friction commonly induced by cryptographic security products.

Underlying these capabilities is an innovative cryptographic protocol, *MaxKyber*, that enables rapid, modular replacement of classical cryptographic protocols that are vulnerable to attack with quantum computers with secure PQC algorithms, supporting key aspects of connected operations. The *MaxKyber* protocol has been formally verified using both Tamarin and ProVerif (120 security properties), undergone expert cryptographic review with all concerns resolved, and been implemented in FPGA hardware with all cryptographic operations executing on fabric.

The enterprise *Ambit Client VPN* platform provides a zero-trust architecture with VPP/DPDK high-performance networking achieving nanosecond latencies and full line rate.

The result is a platform that increases the reliability, resiliency, efficiency, and maintainability of cybersecurity solutions while providing the secure, high-performance communications infrastructure needed to protect remote workers, on-premises networks, cloud deployments, and more.

10 References

[1] See: https://media.defense.gov/2022/Sep/07/2003071834/-1-/1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[2] Registered trademark of American Binary, Inc.

[3]Examples of information with long-term value include financial and transactional information, intellectual property, medical data, and personally identifiable information (PII) that could support identity theft.

[4]See: https://www.keyfactor.com/blog/harvest-now-decrypt-later-a-new-form-of-attack/

[5] See: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved; the standards in question are: FIPS 203, *Module-Lattice-Based Key Encapsulation Mechanism Standard*, FIPS 204, *Module-Lattice-Based Digital Signature Standard*, and FIPS 205, *Stateless Hash-Based Digital Signature Standard*.

[6] See: https://www.cloudflare.com/learning/network-layer/what-is-tunneling/

[7] CNSA 2.0 algorithms have been assessed as sufficient for post-quantum resistance without requiring hybrid constructions.

[8] Specific algorithms included in *Ambit Client VPN* are FIPS 203, *Module-Lattice Key Encapsulation Mechanism* (ML-KEM-1024), AES-256 operating in Galois Counter Mode (GCM), and SHA-512/256.

[9] See: https://s3-docs.fd.io/vpp/25.02/aboutvpp/scalar-vs-vector-packet-processing.html

[10] In a post-quantum secure manner using ML-KEM-1024 key encapsulation.

[11] In-session key rotation is the process of replacing encryption keys with new ones on a regular basis or after a certain amount of data has been transferred.

[12] The maximum transmission unit (MTU) is the largest size, in bytes, of a frame or packet that can be transmitted across a data link. For Ethernet networks using the Internet Protocol (IP), the standard MTU size is 1,500 bytes. Jumbo frames (MTU up to 9000) are only available in specific networking environments such as datacenters.