AMERICAN BINARY

Version: 1.0.4 | **Date:** 2 DEC 2024

Ambit Client: A VPN Solution Employing a Modular Post-Quantum Cryptographic Protocol

American Binary, Inc.
11335 NE 122nd Way Suite 105
Kirkland, WA 98034
e: info@ambit.inc | 1 (408) 827-8822 | w: ambit.inc

Table of Contents

Table of Figures

Table of Tables

1 Executive Summary

Ambit Client VPN combines post-quantum cryptography (PQC) with networking improvements to mitigate both the cryptographic security impacts of quantum computing 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 primitives anticipated to be vulnerable to quantum computers with secure PQC algorithms within a framework extensible to currently ubiquitous network protocols (e.g., Transport Layer Security (TLS), IPSec IKEv2) as well as the generation of a product suite supporting all aspects of connected business operations.

2 Introduction

Quantum computing poses an existential threat to the cryptography that secures the modern connected ecosystem. Generally available, 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 a 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[1]; and

- Once decrypted, they will be able to exploit the information to their benefit.

[1] 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.

This activity is known as a Harvest-Now-Decrypt-Later (HNDL) attack[2], and is ongoing on a broad, prolific, and pervasive scale at the time of this paper's writing. The premise behind the HNDL obsoletes current 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).[3]

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 paucity 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 security protocol. The paper also provides a detailed description of the *MaxKyber®* key establishment process.

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[4] 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

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

[3] 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*.

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

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. Such information may include Personally Identifiable Information (PII), websites and IP addresses visited, or physical location. Privacy involves volitional control over the collection and use of personal information (such as when an employee is working over airport or coffee shop Wi-Fi), whereas security protects the data. 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. This friction means that additional time is required to perform the same amount of work, which translates into higher financial and opportunity costs. 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. As noted in section 1, above, 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.[5]

[5] In 2022, the United States National Security Agency (NSA) issued the Commercial National Security Algorithm Suite, version 2.0 (CNSA 2.0; see: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF). CNSA 2.0 specifically identified six cryptographic algorithms as sufficient for providing post-quantum cryptographic resistance. These included CRYSTALS-Dilithium (ML-DSA), CRYSTALS-Kyber (ML-KEM), the Advanced Encryption Standard (AES) with 256-bit keys, the Secure Hash Algorithm (SHA) with 384- or 512-bit outputs, the Leighton-Micali Signature (LMS) scheme, and the Xtended Merkle Signature Scheme. In April 2024, the NSA issued a clarifying Frequently Asked Questions (FAQ) companion document for CNSA 2.0 (see: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/1/CSI_CNSA_2.0_FAQ_.PDF) that stated in pertinent part: *RSA and Elliptic Curve Cryptography are the main algorithms that need to be replaced to achieve quantum resistance*.

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.[6] 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).[7]

An architectural overview of the *Ambit Client VPN* is provided below.

3.1 *Ambit Client VPN* Architectural Overview

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

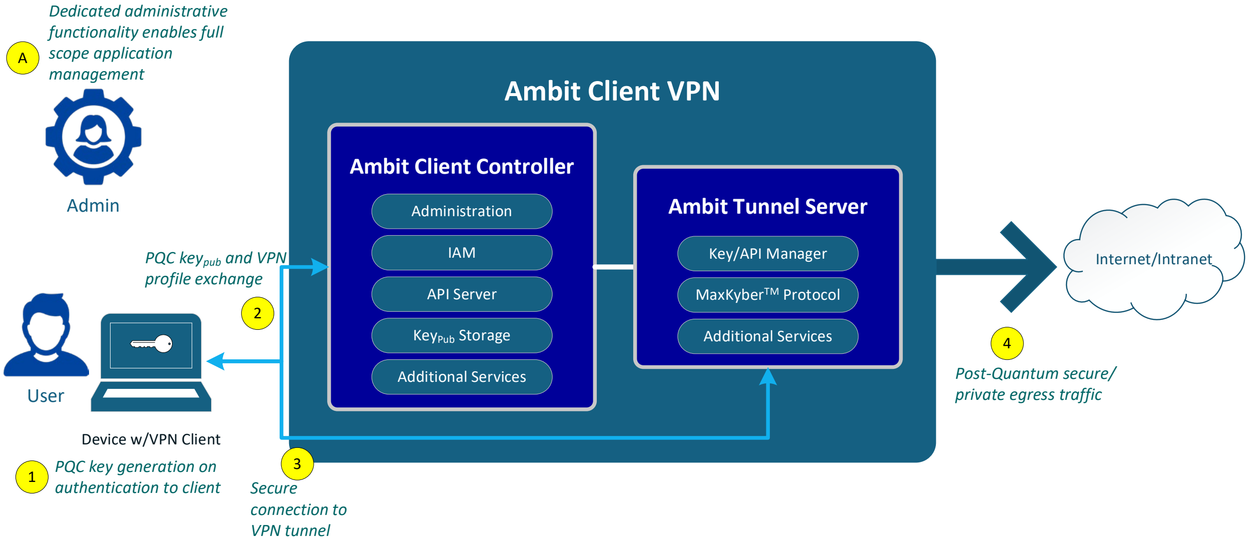
A
Dedicated administrative functionality enables full scope application management
Admin
Ambit Client VPN
Ambit Client Controller
Administration
IAM
API Server
Key$_{Pub}$ Storage
Additional Services
Ambit Tunnel Server
Key/API Manager
MaxKyber^{TM} Protocol
Additional Services
Internet/Intranet
PQC key$_{pub}$ and VPN profile exchange
2
User
Device w/VPN Client
1
PQC key generation on authentication to client
3
Secure connection to VPN tunnel
4
Post-Quantum secure/ private egress traffic

Figure 1, Ambit Client VPN Architectural Overview

Ambit Client VPN comprises three primary components:

- A **client application** that runs on endpoints 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

[6] Specific algorithms included in *Ambit Client VPN* are FIPS 203, *Module-Lattice Key Encapsulation Mechanism*; ML-KEM), and AES-256 operating in Galois Counter Mode (GCM).
[7] See: https://s3-docs.fd.io/vpp/25.02/aboutvpp/scalar-vs-vector-packet-processing.html

- 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, 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.

The ATS comprises three major subcomponents, a combined key and API manager, the *MaxKyber®* protocol, 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.

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

3.2 *Ambit Client VPN* Operational Sequence

The *Ambit Client VPN* functional architectural overview is reprinted here for ease of reference. Attention is directed to the numbered yellow circles that indicate operational sequencing.

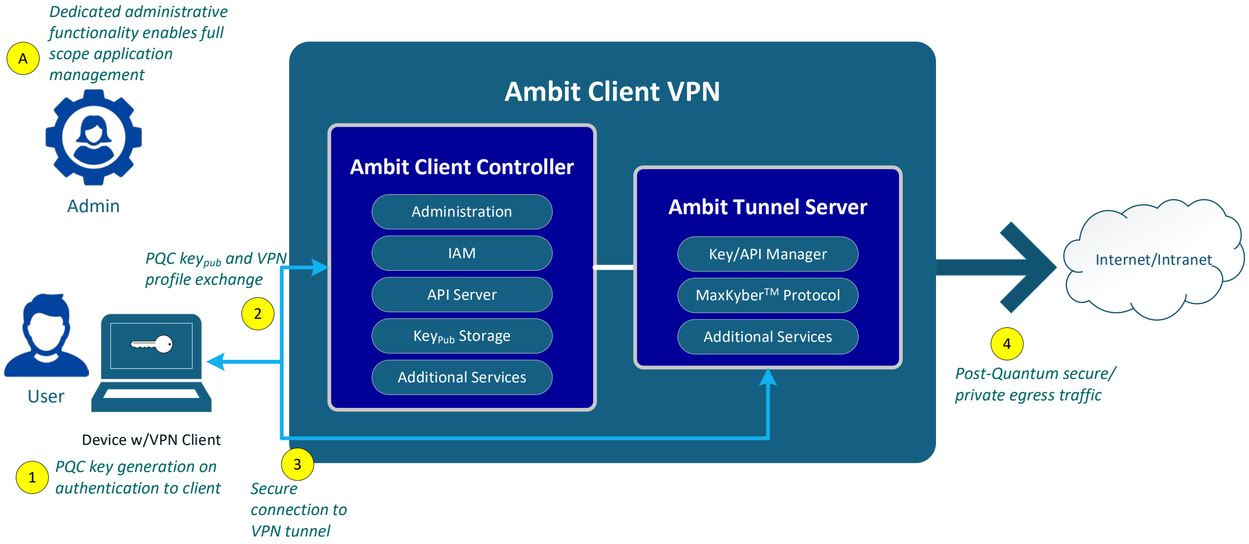
A
Dedicated administrative functionality enables full scope application management
Admin
Ambit Client VPN
Ambit Client Controller
Administration
IAM
API Server
Key$_{Pub}$ Storage
Additional Services
Ambit Tunnel Server
Key/API Manager
MaxKyber^{TM} Protocol
Additional Services
Internet/Intranet
PQC key$_{pub}$ and VPN profile exchange
2
User
Device w/VPN Client
1
PQC key generation on authentication to client
3
Secure connection to VPN tunnel
4
Post-Quantum secure/ private egress traffic

Figure 2, Ambit Client VPN Operational Sequence

Table 1, Ambit Client VPN Operational Sequence

Step	Operational Event
A	*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 keypair. The client application enables the user to initiate a connection to the VPN.
2.	Upon connection initiation, ML-KEM public keys and the parameters for the interaction between the client and the tunnel server, referred to the as the VPN profile, are created.
3.	Once the VPN profile is established, it is used within the context of the *MaxKyber®* protocol to securely establish symmetric keys[8] 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.

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

The *MaxKyber®* protocol is described in the following section.

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

[8] In a post-quantum secure manner.

(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[9], 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.[10] 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 TLS and IPSec IKEv2, thus offering a short path to rapid, prolific PQC adoption.

An architectural overview of the *MaxKyber®* protocol is provided below.

[9] 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.

[10] The maximum transmission unit (MTU) is the largest size, in bytes or octets (eight-bit 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. This value represents the payload of an Ethernet frame and does not include the Ethernet header (typically 18 or 20 bytes, depending on whether 802.1Q VLAN tagging is used). The MTU represents the theoretical maximum amount of data that can be transmitted at the data link layer without fragmentation. Jumbo frames (MTU up to 9000) are only available in specific networking environments such as datacenters.

4.1 *MaxKyber®* Architectural Overview

Figure 3, below portrays the *MaxKyber®* functional architecture:

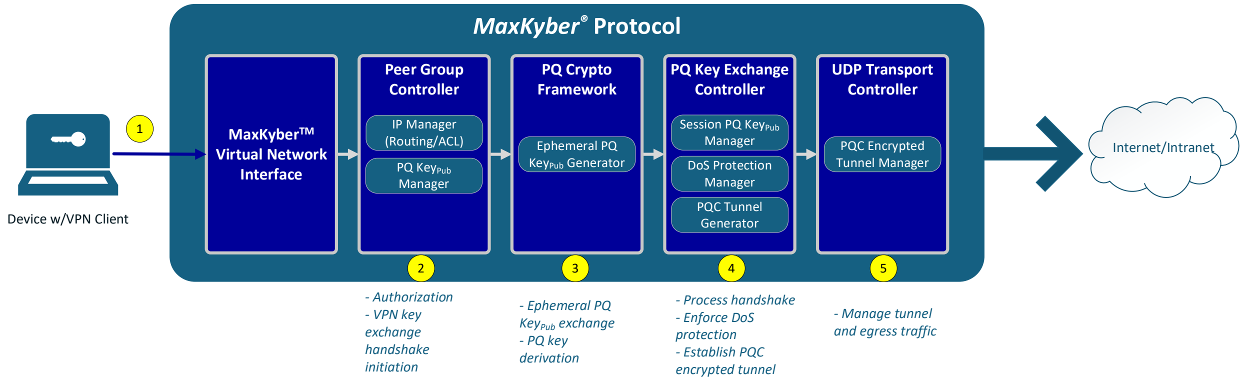
MaxKyber® Protocol
Device w/VPN Client
1
MaxKyber™ Virtual Network Interface
Peer Group Controller
IP Manager (Routing/ACL)
PQ Key$_{Pub}$ Manager
PQ Crypto Framework
Ephemeral PQ Key$_{Pub}$ Generator
PQ Key Exchange Controller
Session PQ Key$_{Pub}$ Manager
DoS Protection Manager
PQC Tunnel Generator
UDP Transport Controller
PQC Encrypted Tunnel Manager
Internet/Intranet
2
3
4
5
- Authorization
- VPN key exchange handshake initiation
- Ephemeral PQ Key$_{Pub}$ exchange
- PQ key derivation
- Process handshake
- Enforce DoS protection
- Establish PQC encrypted tunnel
- Manage tunnel and egress traffic

Figure 3, 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;
- A **post-quantum cryptographic framework** that generates post-quantum public keys and assists with key derivation;
- A **post-quantum key exchange controller** that manages session keys, provides denial-of-service (DoS) attack protection, and generates the post-quantum cryptographic tunnels between clients and the tunnel server; and
- A **User Datagram Protocol (UDP) Transport Controller** that manages tunnels in use.

The peer group controller comprises two major subcomponents: The IP manager and the post-quantum public key manager.

The post-quantum cryptographic framework includes an ephemeral post-quantum public key generator.

The post-quantum key exchange controller includes three major subcomponents: A session post-quantum public key manager, a DoS protection manager, and a PQC tunnel generator.

The UDP transport controller includes a tunnel manager.

The *MaxKyber®* protocol operational sequence is described below.

4.2 *MaxKyber®* Protocol Operational Sequence

The sequence diagram shown in Figure 4, below illustrates the *MaxKyber®* protocol operational sequence.

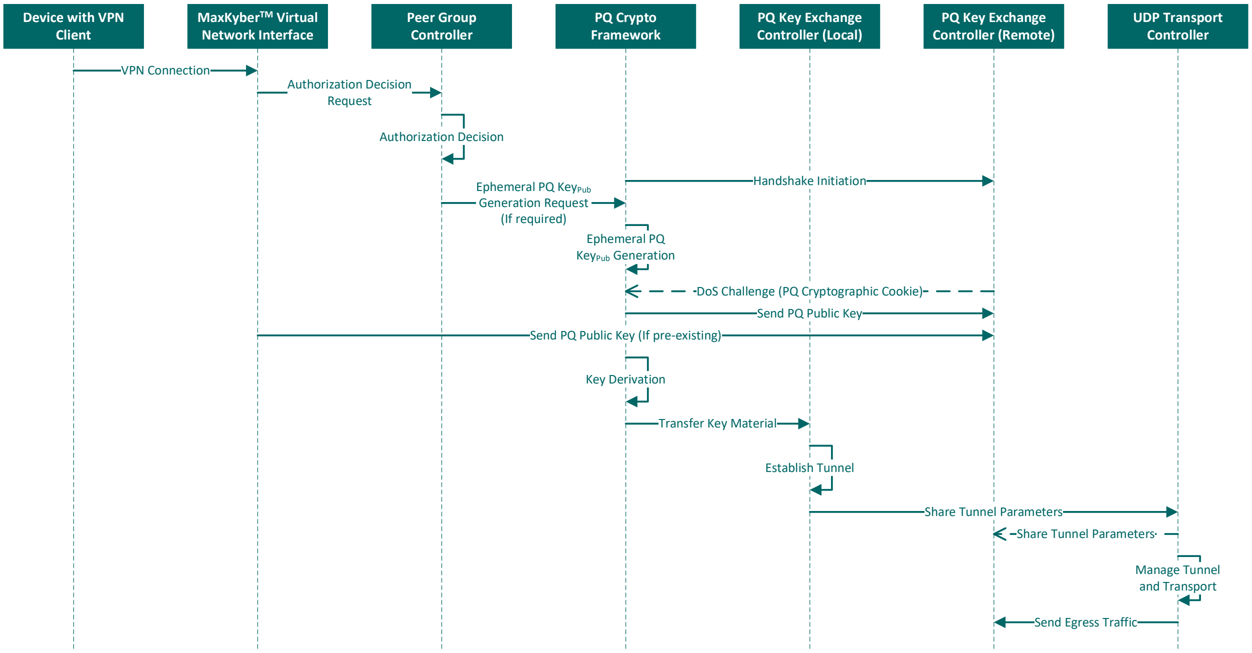
Device with VPN Client
MaxKyber™ Virtual Network Interface
Peer Group Controller
PQ Crypto Framework
PQ Key Exchange Controller (Local)
PQ Key Exchange Controller (Remote)
UDP Transport Controller
VPN Connection
Authorization Decision Request
Authorization Decision
Handshake Initiation
Ephemeral PQ Key_{Pub} Generation Request (If required)
Ephemeral PQ Key_{Pub} Generation
DoS Challenge (PQ Cryptographic Cookie)
Send PQ Public Key
Send PQ Public Key (If pre-existing)
Key Derivation
Transfer Key Material
Establish Tunnel
Share Tunnel Parameters
Share Tunnel Parameters
Manage Tunnel and Transport
Send Egress Traffic

Figure 4, MaxKyber® Operational Sequence

Table 2, MaxKyber® Operational Sequence

Step	Operational Event
1.	An endpoint device with the *Ambit Client VPN* client application attempts to connect to the *MaxKyber®* protocol.
2.	The *MaxKyber®* protocol virtual network interface receives the connection request and forwards it to the peer group controller for an authorization decision.
3.	If the connection request is authorized, the local post-quantum cryptographic framework initiates a handshake with the remote system's post-quantum key exchange controller.
4.	If necessary, the peer group controller requests the generation of an ephemeral post-quantum public key.

5.	If necessary, the post-quantum cryptographic framework generates the ephemeral post-quantum public key.
6.	If necessary, the remote system’s post-quantum key exchange controller sends a post-quantum cryptographic cookie as a DoS challenge.
7.	If necessary, the post-quantum cryptographic framework sends the new post-quantum public key to the remote system’s post-quantum key exchange controller; if the new key is not needed, the virtual network interface sends an existing post-quantum public key.
8.	The post-quantum cryptographic framework conducts key derivation activities.
9.	The post-quantum cryptographic framework transfers the key material to the local post-quantum key exchange controller.
10.	The post-quantum key exchange controller establishes the secure tunnel and shares the tunnel parameters with the UDP transport controller.
11.	The UDP transport controller ensures that the tunnel parameters are shared with the remote system.
12.	The UDP transport controller continuously manages the tunnel and sends secured egress traffic to the remote system.

If the core of *Ambit Client VPN* is the *MaxKyber®* protocol, the *MaxKyber®* protocol’s core is its key establishment (encapsulation) process, which enables secure communication sessions without the risks inherent to transporting sensitive information across insecure channels.

5 Summary of *MaxKyber®* vs Classical Cryptography (ECDH)

Table 3, Summary of MaxKyber® vs Classical Cryptography

Feature	Classical Cryptography (ECDH)	*MaxKyber®* (Post-Quantum)
Security Basis	Elliptic Curve Discrete Logarithm Problem (ECDLP)	Lattice Learning with Errors (LWE)
Quantum Resistance	Vulnerable to quantum attacks	Resistant to quantum attacks
Key Exchange Process	Ephemeral public key exchange	Ciphertext encapsulation and decapsulation
Authentication	Encrypted static keys	Encrypted static keys
Shared Secret Derivation	Scalar multiplication on elliptic curves	Lattice-based encapsulation (ML-KEM CPA & CCA)
Performance	Fast scalar multiplication, compact keys	Efficient lattice computations, compact keys
Forward Secrecy	Provided via ephemeral keys	Provided via ephemeral keys

6 Summary

Ambit Client VPN is among the first of a new generation of VPN products that combine PQC 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 primitives that are vulnerable to attack with quantum computers with secure PQC algorithms within a framework extensible to currently ubiquitous network protocols (e.g., Transport Layer Security (TLS), IPSec IKEv2) as well as the generation of a prolific product suite supporting all aspects of connected business operations.