International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 1317-1325
https://doi.org/10.70917/ijcisim-2026-0977
Article

Quantum-Resistant VPN Protocols for Secure Enterprise Communication

Dipti Yashodhan Sakhare[1], Suvarna Patil[2], Jayamala Kumar Patil[3], Vaishali Sunilsingh Bayas[4], Arjit Tomar[5], Dr. Amol D. Sonawane[6]

[1] Department of Electronics and Telecommunication Engineering, MIT Academy of Engineering, Alandi, Pune, Maharashtra, India.
Email: dipti.sakhare@mitaoe.ac.in
[2] Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, Maharashtra, India.
Email: suvarnapatil@mmcoe.edu.in
[3]Bharati Vidyapeeth's College of Engineering, Kolhapur, Maharashtra, India.
Email: jayamala.p@rediffmail.com
[4] Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune – 411037, Maharashtra, India.
Email: vaishali.bayas1@vit.edu
[5] Department of Computer Science and Engineering, Noida International University, Greater Noida – 203201, Uttar Pradesh, India.
Email: arjit.tomar@niu.edu.in
[6] Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra, India.
Email: amolsonawane1431@gmail.com

Abstract: - The high rate of quantum computing development presents a major threat to the public-key cryptographic technologies that currently form the basis of modern enterprise Virtual Private Network (VPN) networks. Specifically, popular key exchange and authentication models can be attacked with quantum-based cryptanalysis to perform harvest-now, decrypt-later attacks on encrypted enterprise traffic. The design and implementation of quantum-resistant VPN protocols appropriate to enterprise environments in real-world environments are investigated in this paper. The paper gives a thorough discussion of the post-quantum cryptographic primitives, and how these primitives can then be incorporated into the current VPN models using hybrid key establishment protocols that consist of a combination of classical and post-quantum methods. The paper discusses key VPN protocol families, such as IPsec/IKEv2, TLS-based VPNs as well as lightweight tunnel frameworks, and determines useful integration points in the control plane. It suggests a single quantum resistant enterprise VPN architecture with centralized crypto-policy enforcement and key management and monitoring to facilitate crypto-agility and gradual migration. Security and performance analysis indicate that the suggested solution is powerful to overcome the quantum-era threats and maintain the data-plane efficiency and enterprise scalability. These outcomes give a practical roadmap to organizations that are looking to move towards the implementation of post-quantum-secure VPNs without interfering with the current operation of the network.
Keywords: - Quantum-resistant VPN, Post-quantum cryptography, Hybrid key exchange, Enterprise network security, Crypto-agility, Secure tunnel protocols

1. INTRODUCTION

The ongoing high rate of digital transformation of businesses has rendered virtual private networks (VPNs) as an essential part of organizational communication that is safe. The use of VPN protocols like IPsec, TLS based VPNs and light weight tunnel mechanisms is widely utilized to ensure the privacy, integrity and authenticity of data that traverses geographically dispersed corporate infrastructures [1]. The protocols are based on public-key cryptography to perform authentication and exchange keys and use symmetric encryption to carry data. Although this model has been successful against classical computational threat, the emergence of large scale quantum computing has put

cryptography under a paradigm shift with the threat [2]. The most notable result in quantum algorithms is the attack on what is often called a public-key scheme including RSA, Diffie Hellman and elliptic-curve cryptography by quantum algorithms and most notably by Shor. A quantum computer with cryptographically-relevant capabilities can retroactively decrypt past VPN traffic [3] and support so-called harvest-now, decrypt-later attacks. This risk is relevant to businesses especially dealing with sensitive intellectual property, financial documents, healthcare information, and information that the government regulates and have long confidentiality periods. As a result, it has become an immediate need of enterprise network architects to make sure that the current communications based on encryption are resistant to future quantum attackers [4].

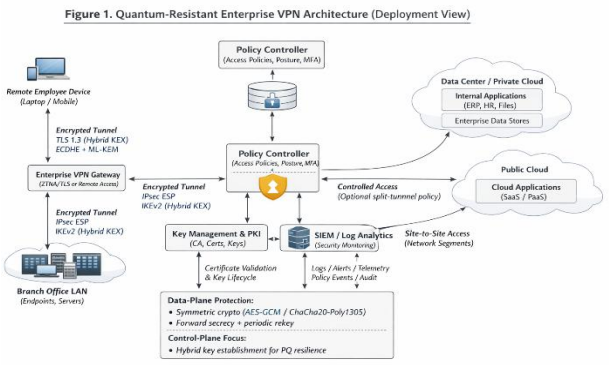

Figure 1. Quantum-Resistant Enterprise VPN Architecture

Post-quantum cryptography (PQC) has become a critical research and standardization field and seeks to create cryptographic primitives which are resistant to classical and quantum attack. Lattice-based, hash-based and code-based algorithms have been found today to be promising candidates in post-quantum security through standardization efforts [5]. Nevertheless, direct substitution of classical cryptographic schemes in enterprise VPNs is not a trivial task as it creates overheads in performance, interoperability, and in the immatureness of the ecosystems deployment as presented in figure 1. Consequently, compounds of cryptography involving both classical and post-quantum key exchange methods are considered to be a viable intermediate measure [6].

2. THREAT MODEL AND SECURITY REQUIREMENTS

The environment of the enterprise VPN implementation is adversarial in nature whereby attackers can have high level of computational power, network, and storage capabilities. When considering quantum-resistant secure communication, the threat model should clearly include the consideration of classical adversaries and the adversaries which are quantum-enabled as well as the transitional phase when hybrid cryptographic systems are used [9]. The main threat that should be taken into account in this paper is a worldwide passive or active network attacker that can monitor, store, alter, inject, or replay VPN packets crossing the public or semi-trusted networks like the Internet or common cloud backbones [10]. The adversary in the quantum setting is also assumed to have - or will eventually have - a cryptographically relevant quantum computer capable of implementing quantum algorithms capable of breaking the traditional public-key primitives [11].

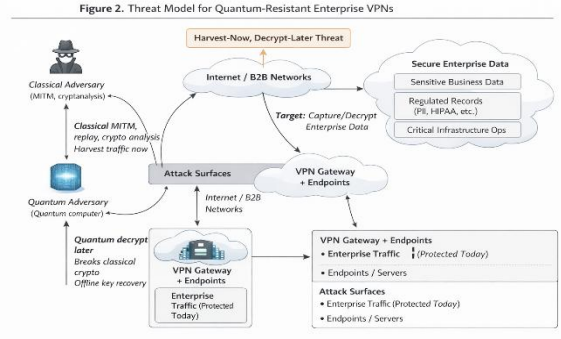

Figure 2. Threat Model for Quantum Resistant Enterprise VPN's

Another very important aspect of the threat model is the harvest-now, decrypt-later scenario. Here, the enemy is not required to steal VPN sessions on the fly. Passively recorded over long durations and stored instead, as represented in figure 2, encrypted traffic can be stored until quantum capabilities develop to the point, at which point historical session keys can be reconstructed in the event that weak key exchange protocols were employed [12]. This risk is extremely high when it comes to enterprise data with high confidentiality periods such as strategic business information, regulated personal data, and sensitive operational communication. According to this threat model, quantum-resistant enterprise VPNs have to meet a number of strict security requirements [13]. Confidentiality is to be maintained on both classical and quantum adversaries ensuring that captured traffic is kept private even with the future cryptanalytic advancements. Forward secrecy is mandatory to reduce the effects of key compromise as well as to avoid retroactive de-encryption of old-recorded sessions [14]. Authentication and integrity guarantees security needs should be resistant to impersonation, as well as manipulation of messages, including immunity against attacks of downgrade, which are attacks that strive to push weaker cryptographic parameters.

3. POST-QUANTUM CRYPTOGRAPHY FOR VPN SYSTEMS

The purpose of post-quantum cryptography (PQC) is to come up with cryptography primitives that are resistant to both classical and quantum adversaries, especially to those who have access to large-scale quantum computers that can implement Shor and Grover algorithms. With respect to enterprise VPN systems, key establishment and authentication protocols are mostly influenced by the use of PQC, and symmetric encryption protocols are mostly compatible with suitable parameter selections [15]. In this section, a more algorithm-centric description of PQC elements of most significance to VPN architectures and how they can be combined with preexisting secure communication protocols is provided.

Step-1]suppose that G is a cyclic group of prime order q having a generator g.

$$Client: a\$Zq, A = ga$$

$$Server: b\$Zq, B = gb$$

Shared classical secret: $Zecdh = gab = Ba = Ab$

Public-key key exchange (RSA and elliptic-curve Diffie-Hellman (ECDH)) algorithms are the most critical weakness of classical VPNs and can be successfully attacked using quantum algorithms. To this end, recent standardization efforts have concentrated on lattice-based key encapsulation mechanisms (KEMs), which are now viewed to be strong candidates of quantum resistance.

Step- 2] ML-KEM (as a KEM) Post-Quantum Key Encapsulation.

A KEM is defined by algorithms: $(pk, sk) \leftarrow KEM.KeyGen()$

$$(c, Kpq) \leftarrow KEM.Encaps(pk)$$

$$Kpq \leftarrow KEM.Decaps(sk, c)$$

In a VPN handshake, the server typically advertises pkS. The client computes:

$$(cpq, Kpq) \leftarrow Encaps(pkS)$$

and sends c_{pq} to the server, which recovers: $Kpq \leftarrow Decaps(skS, cpq)$

ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism) is one of them that has been standardized to provide secure key establishment.

Step-3] Hybrid Key Establishment (Core Model)

Classical secrets with the PQ secrets and a KDF are used to get quantum-resilient session keys. Define an input keying material (IKM) as:

$$IKM = H(Zecdh) \parallel H(Kpq)$$

Optionally bind the transcript to prevent downgrade/mitm:

$$IKM' = IKM \parallel \tau$$

Derive a master secret:

$$Kmaster = HKDF.Extract(salt = 0,\ IKM')$$

Then derive directional traffic keys:

$$kc \to s = HKDF.Expand(Kmaster,\ c2s \parallel \tau,\ L)$$

$$ks \to c = HKDF.Expand(Kmaster, "s2c" \parallel \tau, L)$$

where L is the key length for the chosen AEAD.

In VPN, ML-KEM is not applied separately but rather it is combined with classical key exchange algorithms in a hybrid key establishment model. A classical ephemeral key exchange (e.g. ECDHE) is performed in such designs together with a PQC KEM, with the resultant shared secrets being cryptographically concatenated (typically using a key derivation function) to form the final session keys.

Step-4] Security intuition (hybrid):

Provided that either of the two Zecdh are computationally hidden or Kpq is computationally hidden, then the Kmaster is indistinguishable to random given a set of typical KDF assumptions.

Step-5] Forward Secrecy and Rekeying Model

In order to implement forward secrecy in long-lived tunnels, specify rekey schedule on epochs i=0,1, 2, etc. Let the epoch secret be:

$$Ki = HKDF.Extract(0,\ IKMi')$$

and update with a one-way ratchet:

$Ki + 1 = HKDF.Extract(0,\ H(Ki) \parallel \tau i + 1)1)$

Traffic keys per epoch:

$$kc \to s(i) = HKDF.Expand(Ki, "c2s" \parallel \tau i, L)$$

$$ks \to c(i) = HKDF.Expand(Ki, "s2c" \parallel \tau i, L)$$

This guarantees that Ki does not divulge Kj over j i (backward secrecy) and periodic refreshing cries exposure.

Step-6] Data-Plane Protection (AEAD Model)

As in the case of message mmm and associated data ad (e.g., SPI, sequence number, headers), and nonce n:

$$c = AEAD.Enc(kc \to s(i), n, m, ad)$$

Receiver verifies and decrypts:

$$m \leftarrow AEAD.Dec(kc \to s(i), n, c, ad)$$

If verification fails, output $\perp$.

Step-7] Post-Quantum Authentication (Optional Model)

In case certificates/handshake authentication using PQ signatures is provide:

$$\sigma \leftarrow Sign(sksig, \tau)$$

$$Verify(pksig, \tau, \sigma) \in \{accept, reject\}$$

During transitional deployments, authentication can be classical and key establishment hybrid: the transcript binding τ can be used to avoid algorithm downgrade. This will make sure that even in cases where either the classical or the post-quantum component is compromised, the VPN session will be safe and hence offering a strong transitional security guarantee during the migration period. The post-quantum also needs to be considered in the authentication and digital signatures. RSA or elliptic curve classical signature schemes can be attacked by quantum attacks and there has been interest in lattice-based and hash-based signature schemes. The post-quantum signatures, however, are not as easily implemented in an enterprise PKI setting because of their increased key and signature sizes. Consequently, most VPN architectures have placed hybrid key establishment as a primary design and full post-quantum authentication at the subsequent migration stages.

4. PROPOSED QUANTUM-RESISTANT ENTERPRISE VPN FRAMEWORK

At the center of the structure is a hybrid cryptographic control plane which performs authentication, key establishment and policy enforcement as illustrated in figure 3 below, Setting up a tunnel has a negotiation of a hybrid key exchange between VPN endpoints that involves a classical ephemeral algorithm (e.g., ECDHE) and a post-quantum key encapsulation mechanism (e.g., ML-KEM).

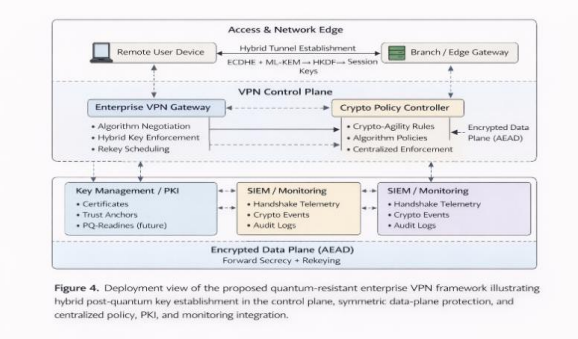

Figure 4. Deployment view of the proposed quantum-resistant enterprise VPN framework illustrating hybrid post-quantum key establishment in the control plane, symmetric data-plane protection, and centralized policy, PKI, and monitoring integration.

Figure 3. Proposed Quantum-Resistant Enterprise VPN Framework

The common secrets resulting are combined using a common key derivation function to come up with session keys. In this design, even the failure of one cryptographic primitive can be contained and hence a threat of harvest-now, decrypt-later is reduced. A centralized crypto policy controller also implements the policies of algorithm choice, downgrade protection, rekey discourse, and crypto-agility using the control plane. The data plane is once again high-throughput secure communication-optimized by application of the known symmetric AEAD algorithms like AES-GCM or ChaCha20-Poly1305. Since in symmetric cryptography quantum attacks are not so significant in combination with proper key sizes, the framework causes minimal disturbance, since the integration of PQC is limited to the control plane. A forward secrecy and optional mechanisms of key ratcheting ensures that the effects of key compromise are reduced anyway because key rekeying is done periodically and key ratcheting is optional. The framework also includes Key Management and PKI services to administer certificates, trust anchors and key lifecycles needed to support operations at the enterprise level. Although early deployments can use classical certificates, the architecture is also not restricted to such in the future, as PKI ecosystems evolve to use post-quantum authentication techniques.

5. SECURITY ANALYSIS

This part will evaluate the security characteristics of the proposed quantum-resistant enterprise VPN model with respect to the adversarial model that has been described in Section 3. The analysis will take into account confidentiality, authentication, forward secrecy, resistance to attacks of quantum scale and operating strength in case of partial breakage of cryptography. It focuses on defense-in-depth as it is understood that enterprises should be secure throughout a long cryptographic transition. The most serious threat the framework is resistant to is the harvest now, decrypt later attack where attackers intercept encrypted VPN traffic and store it to decrypt it in the future using quantum hardware. The risk is addressed in the framework by using a hybrid key creation using classical ephemeral key exchange and post-quantum key encapsulation mechanism. The framework guarantees the long-term confidentiality, even in the event that one cryptographic primitive is subsequently compromised by cryptographically fusing both shared secrets in deriving the key. Moreover, cryptographic parameter binding to the transcript of the handshake gives high-security to prevent man-in-the-middle and downgrade attacks which are used to undermine negotiated security configurations. Table 1 presents a summary of the requirement of representative threat scenarios to be met by particular security mechanisms within the framework. As is shown in the mapping, the threats to both

the control plane (e.g. key compromise, algorithm downgrade) and the data plane (e.g. replay attacks), are addressed by coordinated cryptographic and policy-based controls.

TABLE 1. THREATS VS. SECURITY MECHANISMS IN THE PROPOSED FRAMEWORK

Threat Scenario	**Attack Description**	**Mitigation Mechanism**	**Framework Component**
Harvest-now, decrypt-later	Passive capture of encrypted VPN traffic for future decryption	Hybrid key establishment (ECDHE + ML-KEM)	VPN Control Plane
Man-in-the-middle (MITM)	Interception and modification of handshake messages	Transcript-bound authentication and key derivation	VPN Gateway
Downgrade attack	Forcing weaker cryptographic algorithms	Centralized crypto-policy enforcement	Crypto Policy Controller
Key compromise	Leakage of long-term or session keys	Ephemeral keys and periodic rekeying	Control & Data Planes
Replay attacks	Reuse of captured packets	AEAD with nonces and sequence numbers	Encrypted Data Plane
Partial algorithm failure	Break in classical or PQ algorithm	Hybrid key derivation ensures resilience	Hybrid KEX Module

The framework aims at meeting an overall set of security attributes which are in line with enterprise and regulatory demands. Forward secrecy is realized by using ephemeral key exchange and a time-based rekeying to minimize the effect of exposure to credentials. Table 2 summarizes these properties and how they are achieved in the framework by establishing a connection between the abstract security requirements and the concrete architectural mechanisms.

TABLE 2. SECURITY PROPERTIES ACHIEVED BY THE PROPOSED VPN FRAMEWORK

Security Property	**Formal Requirement**	**Realization in Framework**
Confidentiality	Resistance to classical and quantum adversaries	Hybrid KEX + AEAD encryption
Forward secrecy	Past session keys remain secure after compromise	Ephemeral key exchange + rekeying
Integrity	Detection of message modification	AEAD-based authenticated encryption
Authentication	Verification of peer identity	Certificate-based or identity-centric control plane
Crypto-agility	Ability to update algorithms and parameters	Policy-driven cryptographic enforcement
Auditability	Visibility into cryptographic operations	SIEM-integrated telemetry and logging

Afraid with AEAD-based encryption, the integrity and authenticity of tunneled data is ensured, whereas authentication is based on either certificate-based or identity-centric control-plane schemes. Notably, the framework focuses on crypto-agility, which allows depreciating and changing the algorithms quickly as a response to new vulnerabilities.

6. PERFORMANCE AND DEPLOYMENT ANALYSIS

The implementation of quantum-resistant VPN systems creates new performance and operational aspects that have to be carefully considered to provide enterprise viability. In contrast to classical VPN upgrades that can be largely software optimization-oriented, post-quantum integration has the greatest effect on the control plane, especially in tunnel establishment and rekeying stage. The anticipated performance overheads, scalability considerations, and deployment issues of the suggested quantum-resistant enterprise VPN framework.

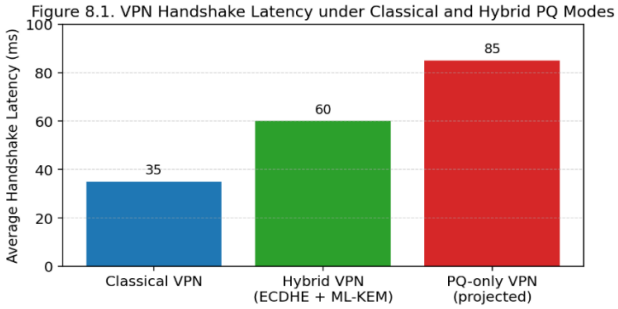

Figure 4. VPN Handshake Latency under Classical and Hybrid PQ Modes

The hybrid key establishment has the greatest performance effect in the short term. The application of post-quantum key encapsulation, i.e. lattice-based KEMs, uses bigger public keys, ciphertexts and handshake messages than classical elliptic-curve exchanges. Subsequently, due to VPN handshakes, more bandwidth is consumed and there is a slight increase in latency particularly during initial set up of tunneling as indicated in figure 4. In the case of enterprise environments where tunnels are frequently created e.g. remote access gateways to serve mobile users, this overhead can be observable on links with high latency or bandwidth limits. Nonetheless, the data plane performance of the established tunnel is not affected much, since the encryption of data using AEAD algorithms remains efficient based on the symmetric algorithm.

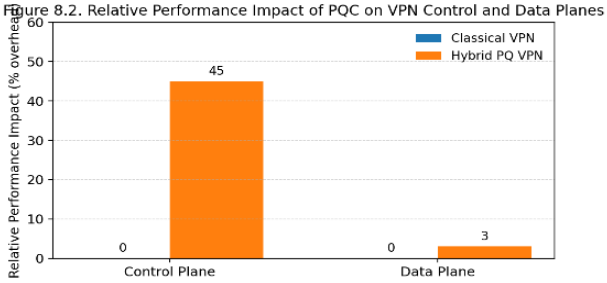

Figure 5. Relative Performance Impact of PQC on VPN Control and Data Planes

Another consideration that is critical is the computational overhead. Although post-quantum algorithms are more computationally-intensive than classical elliptic-curve operations, state-of-the-art server-class machines can execute hybridized key exchanges with no throughput reduction at an effective scale provided they are adequately provisioned as in figure 5. The effect is also alleviated by the fact that the establishment of key takes place rarely as compared to data transmission. In long-lived site-to-site tunnels, the amortized cost of post-quantum operations is small, so IPsec-based enterprise backbones are well suited in this regard.

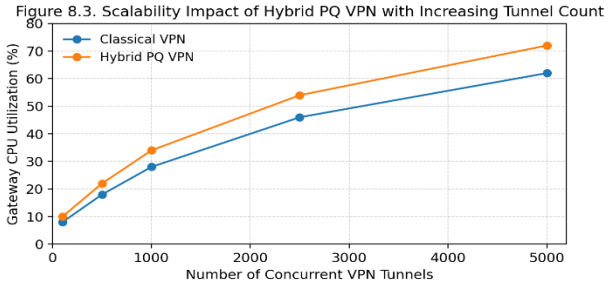

Figure 6. Scalability Impact of Hybrid PQ VPN with Increasing Tunnel Count

Scalabilitywise, such centralized components like the crypto policy controller and key management infrastructure need to be scaled to support more cryptography metadata and handshake telemetry. The use of larger keys and certificates can add an extra burden to the PKI systems and logging pipelines, and careful capacity planning and sampling of the telemetry is required. However, these issues can be handled within the current enterprise monitoring and orchestration systems as depicted in figure 6. The interoperability and the necessity of phased migration are the key factors that cause the complexity of deployments. Businesses can hardly run homogeneous VPNs; rather they use multi-vendor gateways, heterogeneous endpoint devices and hybrid on-premise-cloud infrastructure. The suggested framework will help to manage this fact as it supports crypto-agility and hybrid modes, enabling the use of post-quantum mechanisms on an incremental and selective basis depending on policy, device capability, and risk profile. In the transition period, there can be a co-existence between classical-only tunnels and hybrid tunnels, which means that there is continuity of services at the expense of gradually enhancing quantum resilience.

7. CONCLUSION

This paper has discussed the architecture and implementation of quantum resistant VPNs to provide secure communication between enterprises to respond to the threat of quantum computing on the traditional cryptographic systems. The shift to post-quantum security has turned into a strategic requirement and not just a theoretical consideration as enterprise VPN infrastructures remain very dependent on the use of public-key cryptography to perform authentication and key establishment. As is shown in the analysis, the best and most instantly implementable solution to this problem is the introduction of hybrid cryptographic protocols, which are classical and post-quantum based to provide continuity of protection in the transition period. This paper, by undertaking a methodical assessment of VPN protocol architecture, brings to focus the fact that post-quantum cryptography can be successfully implemented into both site to site and remote access VPN infrastructures. The proposed framework ensures high-performance data-plane functionality without introducing significant changes to the design, and the impact of the control plane ensures high resilience to harvest-now/decrypt-later attacks. The security analysis also confirms that the combination of the establishment of hybrid keys in forward secrecy and the enforcement of centralized crypto-policies will effectively offer very strong defense-in-depth against both classical and quantum era adversaries. According to performance and deployment analysis, though post-quantum integration comes at a quantifiable overhead in terms of tunnel establishment and rekeying, the effect is controllable in an enterprise grade infrastructure. The article can be regarded as a viable, scalable roadmap to enterprises interested in long-term cryptography protection in the post-quantum age. The proposed framework by connecting the new post-quantum standards to real-life VPN systems is a strong underlying to the secure, future-proof enterprise communication.

References

1. G. Fitzgibbon and C. Ottaviani, “Constrained device performance benchmarking with the implementation of post-quantum cryptography,” Cryptography, vol. 8, no. 2, Art. no. 21, 2024.
2. M. Vidaković and K. Miličević, “Performance and applicability of post-quantum digital signature algorithms in resource-constrained environments,” Algorithms, vol. 16, no. 11, Art. no. 518, 2023.
3. Rubio García, S. Rommel, S. Takarabt, J. J. Vegas Olmos, S. Guilley, P. Nguyen, and I. T. Monroy, “Quantum-resistant transport layer security,” Computer Communications, vol. 213, pp. 345–358, 2024.
4. S. Ullah, J. Choi, and H. Oh, “IPsec for high-speed network links: Performance analysis and enhancements,” Future Generation Computer Systems, vol. 107, pp. 112–125, 2020.
5. A. C. Aguilera, X. A. I. Clemente, D. Lawo, I. T. Monroy, and J. V. Olmos, “First end-to-end PQC-protected DPU-to-DPU communications,” Electronics Letters, vol. 59, Art. no. e12901, 2023.
6. C. Lawo, R. Frantz, A. C. Aguilera, X. A. I. Clemente, M. P. Podleś, J. L. Imaña, I. T. Monroy, and J. J. V. Olmos, “Falcon/Kyber and Dilithium/Kyber network stack on NVIDIA’s data processing unit platform,” IEEE Access, vol. 12, pp. 38048–38056, 2024.
7. L. Malina, S. Ricci, P. Dobiaš, P. Jedlička, J. Hajný, and K. R. Choo, “On the efficiency and security of quantum-resistant key establishment mechanisms on FPGA platforms,” in Proc. 19th Int. Conf. Security and Cryptography (SECRYPT), Lisbon, Portugal, Jul. 2022, pp. 605–613.
8. M. Liao, S. Zheng, S. Pan, D. Lu, W. He, G. Situ, and X. Peng, “Deep-learning-based ciphertext-only attack on optical double random phase encryption,” Opto-Electronic Advances, vol. 4, Art. no. 200016, 2021.
9. O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem, H. M. El-Hoseny, H. S. El-Sayed, and A. M. Abbas, “Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform,” Optical and Quantum Electronics, vol. 53, Art. no. 1, 2021.
10. G. Qu, W. Yang, Q. Song, Y. Liu, C.-W. Qiu, J. Han, D.-P. Tsai, and S. Xiao, “Reprogrammable meta-hologram for optical encryption,” Light: Science & Applications, vol. 9, Art. no. 1, 2020.

11. T. Liu, Z. Han, J. Duan, and S. Xiao, “Phase-change metasurfaces for dynamic image display and information encryption,” Physical Review Applied, vol. 18, 2022.
12. R. Cohen, E. Wohlgemuth, Y. Yoffe, Y. Yalinevich, I. Attia, A. Yalinevich, R. Yehoash, A. Rabinovich, and D. Sadot, “Cryptanalysis of practical optical layer security based on phase masking of mode-locked lasers and multi-homodyne detection,” Journal of Lightwave Technology, vol. 42, no. 1, pp. 167–182, 2024.
13. P. McKenna and L. Torres, “Practical implementation of quantum key distribution in coherent optical networks,” Quantum Information Processing, vol. 22, pp. 234–250, 2023.
14. F. Hu, L. Lamata, C. Wang, X. Chen, E. Solano, and M. Sanz, “Quantum advantage in cryptography with a low-connectivity quantum annealer,” Physical Review Applied, vol. 13, Art. no. 054062, 2020.
15. M. A. R. Tungar and D. Deshpande, “Review paper on Secure and Efficient Framework for Big Data Storage and Access Control in Cloud Environments Using Optimized Cryptographic Algorithms”, IJRAET, vol. 14, no. 2s, pp. 14–18, Dec. 2025.