

Post-Quantum Secure Datacenter Interconnect

Problem statement

The security of modern network communication relies heavily on public-key cryptographic schemes used for key exchange and authentication. Widely deployed algorithms such as RSA and elliptic-curve cryptography (ECC) are considered secure against classical computing attacks but are expected to become vulnerable in the presence of sufficiently powerful quantum computers.

This creates a fundamental long-term risk: data transmitted today may be intercepted, stored, and decrypted in the future once quantum-capable adversaries become available. For datacenter interconnects carrying sensitive workloads, such as storage replication, internal services, and distributed computation, this ***“harvest now, decrypt later”*** threat represents a critical concern.

In response, post-quantum cryptography (PQC) has emerged as a new class of algorithms designed to remain secure against quantum attacks. Recent standardization efforts, including NIST-selected algorithms such as ML-KEM (Kyber, NIST FIPS 203) and ML-DSA (Dilithium, NIST FIPS 204), provide a foundation for deploying quantum-resistant communication systems.

However, adopting post-quantum cryptography in high-speed network environments introduces significant practical challenges:

- **High computational complexity**

Post-quantum key exchange mechanisms are substantially more demanding than traditional cryptographic schemes, increasing processing requirements for session establishment and key rotation.

- **Software scalability limitations**

Implementing PQC in software places a heavy burden on host CPUs, making it difficult to sustain high-throughput operation at modern datacenter link speeds.

- **Lack of flexible hardware support**

Existing ASIC-based networking and security solutions typically do not support post-quantum algorithms, and their fixed-function nature limits their ability to adapt to evolving cryptographic standards.

- **Performance constraints at line rate**

Combining high-speed packet processing with advanced cryptography, especially in a way that preserves low latency and predictable behavior, remains a key technical challenge.

As a result, there is a **growing gap between the availability of quantum-resistant cryptographic algorithms and the ability to deploy them efficiently in real-world, high-performance networking environments.**

This creates the need for a new approach that enables:

- deployment of post-quantum secure communication at datacenter link speeds,
- minimal impact on latency and network behavior,
- independence from host CPU resources,
- and flexibility to integrate evolving cryptographic standards.

DYNANIC addresses these challenges by enabling hardware-accelerated, inline post-quantum encryption directly within the network data path, allowing datacenter interconnects to operate at line rate while maintaining long-term cryptographic security and eliminating dependence on host CPU resources completely.

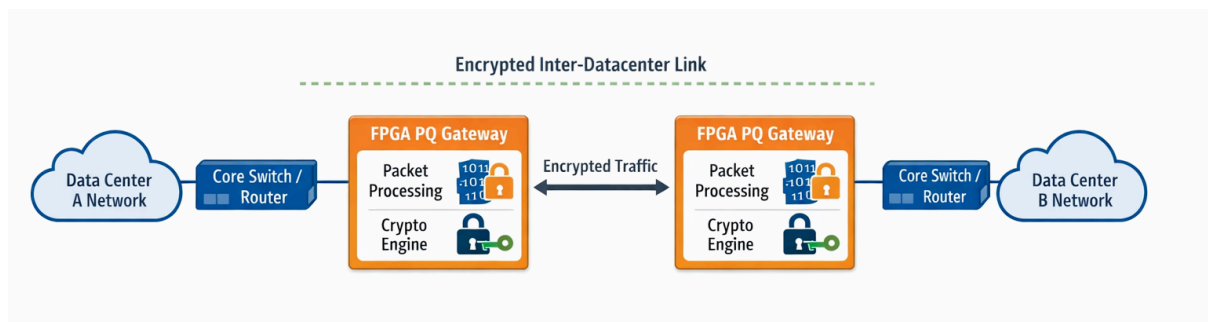
Solution description

The offered DYNANIC PQC solution introduces a hardware-accelerated architecture for post-quantum secure datacenter interconnects, where cryptographic processing is performed directly within the network data path.

At its core, the solution leverages a programmable FPGA-based SmartNIC that integrates packet processing and cryptographic functions into a single, unified datapath pipeline. Network traffic is processed in-line as it traverses the interface, enabling encryption and decryption to occur at line rate without involving host CPU resources.

Unlike traditional approaches, this architecture does not rely on software-based encryption or external security appliances. Instead, all critical operations, including packet classification, tunnel association, key management, and data encryption, are executed within the SmartNIC hardware. This ensures predictable latency, eliminates CPU bottlenecks, and enables consistent performance even at high link speeds such as 100G, 200G, and 400G. Furthermore, all the cryptographic data (e.g. established keys) are completely isolated in the hardware, never being accessible from the host.

The solution is deployed as an inline element within the network path, enabling secure communication between datacenter locations without requiring changes to applications.



As shown in the figure, the SmartNIC-based system operates as a transparent “bump-in-the-wire” node positioned between network segments. Traffic entering the device is processed in real time, associated with a secure tunnel, and forwarded after encryption or decryption—without requiring host-level intervention.

The internal architecture is based on a structured, multi-stage processing pipeline:

- **Packet processing and flow identification**

Incoming packets are parsed in real time, with key header fields extracted and used to identify flows and associate traffic with secure tunnels.

- **Session management and key handling**

Secure sessions are established using post-quantum key exchange mechanisms, with session keys stored and managed directly within the SmartNIC hardware. This ensures that sensitive key material remains isolated from the host system.

- **Inline cryptographic processing**

Once a packet is associated with a secure session, payload encryption or decryption is performed in-line using hardware-accelerated authenticated encryption algorithms. This allows traffic to be processed at wire speed in each direction while maintaining strong security guarantees.

- **Forwarding and transparent integration**

After processing, packets are forwarded to the output interface with minimal additional latency. The system operates transparently within the network, preserving existing traffic flows and routing behavior.

This tightly integrated pipeline allows the system to maintain full throughput while introducing only minimal and deterministic latency overhead.

A key aspect of the architecture is its ability to support post-quantum cryptographic algorithms alongside high-speed data encryption. Post-quantum key exchange mechanisms are integrated into the control and session layer, enabling secure tunnel establishment and periodic re-keying without disrupting ongoing traffic.

At the same time, symmetric authenticated encryption is implemented in a highly parallelized hardware pipeline, ensuring efficient processing of high packet rates across a wide range of traffic profiles.

Thanks to the reconfigurable nature of FPGA technology, the solution remains adaptable to evolving cryptographic standards. New algorithms, protocol extensions, or security features can be integrated without requiring changes to the underlying hardware platform. This provides a future-proof foundation for long-term deployment in environments where both performance and cryptographic agility are critical.

Key Advantages

The proposed architecture delivers a unique combination of security, performance, and flexibility, enabling practical deployment of post-quantum secure communication in high-speed datacenter environments.

- **Inline Post-Quantum Encryption at Line Rate**
Encryption and decryption are performed directly within the network data path, allowing secure communication at 100G, 200G, and 400G link speeds without impacting throughput or requiring external appliances.
- **Quantum-Resistant Security by Design**
Integration of post-quantum key exchange mechanisms ensures long-term protection against emerging quantum threats, eliminating the risk of future decryption of intercepted data.
- **CPU Offload and System Efficiency**
All cryptographic operations are executed within the SmartNIC hardware, removing the burden from host CPUs and enabling more efficient utilization of compute resources for application workloads.
- **Deterministic Low Latency**
The hardware pipeline introduces only minimal and predictable latency, making the solution suitable for latency-sensitive environments such as distributed systems and real-time services.
- **Hardware-Isolated Key Management**
Cryptographic keys are generated, stored, and processed within the SmartNIC, reducing exposure to host-level vulnerabilities and minimizing the attack surface.
- **Seamless Integration into Existing Infrastructure**
The solution operates as a transparent inline element, allowing deployment without changes to applications, servers, or higher-layer network configurations.
- **Scalable to Future Network Speeds**
The architecture scales with available hardware resources and supports increasing link speeds through parallel processing and pipeline optimization.
- **Adaptable to Evolving Cryptographic Standards**
Thanks to the reconfigurable nature of FPGA technology, the system can integrate new cryptographic algorithms and protocol updates without hardware replacement, ensuring long-term viability.

Value for Customers

The proposed architecture enables organizations to deploy quantum-resistant security without compromising performance, operational simplicity, or infrastructure efficiency. By integrating cryptographic processing directly into the network data path, the solution delivers both immediate and long-term value across multiple dimensions.

Future-Proof Security for Critical Data

Organizations can protect sensitive data against future quantum threats today, ensuring long-term confidentiality for workloads such as storage replication, backup, and inter-datacenter communication.

Elimination of Performance-Security Trade-offs

Unlike traditional approaches, the solution enables strong cryptographic protection at full line rate, removing the need to choose between security, throughput, and latency.

Reduced Infrastructure Complexity

By operating as an inline element within the existing network path, the solution eliminates the need for dedicated encryption appliances, additional network hops, or complex architectural changes.

Lower Compute Resource Consumption

Offloading cryptographic processing from CPUs reduces server load, allowing existing infrastructure to handle higher traffic volumes or freeing resources for application and AI workloads.

Operational Transparency

The system integrates seamlessly into existing environments without requiring changes to applications, routing, or higher-layer protocols, minimizing deployment risk and operational overhead.

Scalable Deployment Model

The architecture can be deployed incrementally – starting with selected interconnects and expanding across the infrastructure – allowing organizations to align security investments with actual needs.

Long-Term Investment Protection

The use of programmable hardware enables continuous adaptation to evolving cryptographic standards and protocols, reducing the risk of hardware obsolescence and extending the lifecycle of deployed systems.



Experience Unmatched Network Efficiency
www.dyna-nic.com

Need more information?

Feel free to contact us at info@dyna-nic.com

For more information visit www.dyna-nic.com