

PQC and QKD Migration Network with PUF-based Service Authentication

Konstantinos Krilakis✉
kostaskrilak@di.uoa.gr
National and Kapodistrian University
of Athens
Athens, Greece

Antonia Tsili
tonia.tsili@eulambia.com
Eulambia Advanced Technologies Ltd.
Athens, Greece

Aikaterini Mandilara
aikaterini.mandilara@eulambia.com
Eulambia Advanced Technologies Ltd.
Athens, Greece

Maya Thabet
mthabet@di.uoa.gr
National and Kapodistrian University
of Athens
Athens, Greece

Dimitris Syvridis
National and Kapodistrian University
of Athens
Athens, Greece

Abstract

We present an enterprise-grade, service-oriented network infrastructure for quantum-safe communication, enriched with stateless authentication based on physical unclonable functions (PUFs) for external services. Building on a readily deployable system that secures the distribution of keys derived from multi-vendor QKD (or other sources) through an independent, cloud-based, PQC-driven identity and trust management, we demonstrate the infrastructure's extensibility by introducing the External Service Provisioner (ESP) and external target services. The ESP allows clients and services to authenticate against the infrastructure using nonce-bound PQC signatures reconstructed via PUFs, removing the need for stored long-term keys.

CCS Concepts

• **Security and privacy** → **Network security; Authentication; Access control; Authorization**; • **Networks** → **Network architectures; Network services; Cloud computing; Network management**.

Keywords

QKD, PQC, Quantum-secure communications, Post-quantum networking, Secure quantum networks, Quantum network architectures, PUF, KMS, IAM

ACM Reference Format:

Konstantinos Krilakis, Antonia Tsili, Aikaterini Mandilara, Maya Thabet, and Dimitris Syvridis. 2026. PQC and QKD Migration Network with PUF-based Service Authentication. In *Proceedings of ACM Conference on Post-Quantum and Quantum-based Security (PQQS '26)*. ACM, New York, NY, USA, 7 pages. <https://doi.org/XXXXXXX.XXXXXXX>

*All authors contributed equally to this research.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

PQQS '26, San Jose, CA

© 2026 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-XXXX-X/2026/11
<https://doi.org/XXXXXXX.XXXXXXX>

1 Introduction

Quantum key distribution (QKD) and post-quantum cryptography (PQC) stand as two emerging frontiers in cybersecurity [6], each carrying its own trade-offs. How well each approach can be adopted depends on its adaptability to both legacy and modern infrastructures. As both technologies mature, research focus is gradually shifting away from novel cryptographic primitives secure against quantum adversaries and toward solutions that ease network migration to fully quantum-safe infrastructures. This transition calls for approaches that make optimal use of whatever quantum-secure technology is readily available, remain crypto-agile enough to accommodate standards updates, and integrate seamlessly into existing systems while protecting every link.

QKD offers a means of exchanging cryptographic keys with security that is unconditional in principle [21]. Operating at the network's physical layer, its basic configuration links two terminals, conventionally named Alice and Bob, over a dedicated dark fibre of restricted length. Clients at either end obtain symmetric keys only once they gain authorised, secure access to the corresponding terminal. Because this arrangement is inherently pairwise, both its range of application and its scalability are tightly constrained, an issue compounded by the high cost of the hardware involved. Under suitable assumptions, this limitation can be partly addressed by chaining QKD links through trusted nodes (TNs) [15], letting symmetric keys reach clients at the outer ends of a sequence of pairs and pushing key agreement beyond a single link's distance ceiling. This comes at a price – each additional QKD node adds further cost, and keys can only pass between clients attached to nodes within that particular chain, at a bounded rate.

This is where PQC enters the picture. Being software-based, it fits more readily into existing systems and mitigates the scalability issues inherent to QKD, while still safeguarding communications against quantum attacks. The emergence of readily adoptable PQC Key Encapsulation Mechanisms (KEMs) and digital signature algorithms has prompted a broad revision of network standards worldwide, particularly in critical domains such as defence and government. However, the newly standardised algorithms and standardisation candidates remain scarcely available in commercial devices, which hinders their integration into existing applications

and protocols and, in turn, limits real-world experimentation and large-scale deployment.

Since QKD requires an authenticated classical channel to prevent man-in-the-middle (MIM) attacks, PQC algorithms have been widely explored as a practical replacement for the pre-shared symmetric keys traditionally used for authentication [9, 18, 19, 22]. In parallel, Physical Unclonable Functions (PUFs) [14] have emerged as a promising alternative. By exploiting random manufacturing variations to generate unique, unclonable hardware fingerprints, PUFs enable device-level authentication without storing long-term secret keys. However, when used as the primary authentication mechanism for QKD, they require a dedicated authentication infrastructure in place of the mature Public Key Infrastructure (PKI) trust model. Here, we introduce an extensible security-as-a-service networking system providing KMS services to authenticated and authorized clients, and acting as an individual security layer for the identification and authentication of network entities (NEs) connected to a multi-domain topology. This is accomplished by leveraging PQC, QKD and PUFs under cloud management that is enriched with the External Service Provisioner (ESP), which lets the KMS act as a secure service provisioner and adds an authentication function to services beyond the existing enterprise-grade infrastructure. Post-quantum methods are employed to securely conduct the provision of secret key material – that could be provided via QKD or PUFs – and other cryptographic services, over classical channels. As a result, the need for extensive QKDN installations is avoided, while exploiting existing QKD pairs and essentially extending quantum-safe key relay in a way compatible to legacy networks. The architecture is organized into separate, autonomous domains with a central supervisor and a target service cloud segment available to all NEs. More specifically, we distinguish the following properties and novelties:

- A native, cross-platform, multi-domain network architecture with support for heterogeneous topologies.
- An agnostic design supported by a zero-touch provisioning (ZTP) driver framework.
- Integration of multi-vendor QKD systems within some domains, combined with PQC KEMs to enable unlimited distance quantum-secure key relay.
- A unified security layer incorporating multi-factor authentication and cloud-based key management for trust, identity, and interoperability.
- SDN-driven automation with detailed telemetry for monitoring and reporting.
- PUF-based client authentication offered as a cloud service through the External Service Provisioner (ESP) demonstrated with both optical and SRAM PUF devices.
- A nonce-based PQC signature reconstruction mechanism that extends PUF-derived trust to target cloud services exposing Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) functions, allowing clients to authenticate without repeated exchange of long-term credentials.

2 Related Work

Attempts to address QKD limitations include the MadQCI approach [12, 13], which integrates SDN within a multi-domain, multi-vendor

QKD testbed. Each domain is orchestrated by an SDN controller and comprises QKD links interconnected through TNs. The architecture remains QKD-centric, with operation driven by quantum link availability and topology, while PQC is used as a complementary mechanism for long-distance emulation and hybrid key generation. Consequently, key distribution relies on TN forwarding and remains tightly coupled to the underlying QKD infrastructure, leading to increased architectural complexity.

Several works have attempted to overcome the scalability issues of QKD through improved key management, hybrid protocols, and practical QKD network deployments. Surveys highlight the need to decouple key generation from key consumption while addressing scalability, synchronization, and multi-vendor interoperability challenges [7]. Other approaches explore key-pool management and provisioning mechanisms for partially deployed QKD networks [20, 23], while additional research incorporates PQC into authentication and TLS to strengthen classical communication channels [3, 10, 17].

Recent research has also demonstrated practical multi-vendor QKD deployments integrating PQC and SDN orchestration [11–13]. Finally, federation architectures have been proposed to interconnect geographically separated QKD infrastructures while maintaining interoperability across heterogeneous environments [4]. However, these approaches remain largely centred on QKD infrastructures and relay coordination. Contrary to Mendez et al. [13], where PQC is used in some segments of a QKDN for emulating long-distance QKD connections, we employ post-quantum methods to securely conduct the provision of secret key material, whether generated via QKD or other means, alongside other cryptographic services, over classical channels. As a result, the need for extensive QKDN installations is avoided, while existing QKD pairs are exploited and quantum-safe key relay is essentially extended in a way compatible with legacy networks.

Separately, physical unclonable functions (PUFs) have been established as a means of deriving device-specific, unclonable identifiers and key material from manufacturing-induced physical randomness. Subsequent work has extended this concept across a range of physical substrates and application domains, including surveys covering PUF-based authentication and communication protocols, their associated challenges, and their applications to IoT security [2]. More recent efforts have focused on strengthening the resilience of low-cost optical PUF implementations against machine-learning-based modelling attacks, demonstrating optimal performance under such adversarial conditions [1]. While these works establish PUFs as a mature, hardware-rooted primitive for identification and key generation individually, their integration as a cloud-orchestrated, service-based authentication layer within a multi-domain, multi-vendor QKD/PQC network, as proposed in this work, remains largely unexplored.

3 Network topology

The proposed work introduces a multi-site enterprise-grade network infrastructure whose service-based design has a two-fold purpose; first, it allows *quantum secure* communication between any NEs involved; second, it offers PUF-authenticated cloud service access to the member NEs, thus switching from a transaction-centred

functionality to a service-oriented platform capable of accommodating arbitrary cloud services beyond key delivery. Our deployment consists of twelve (12) independent network domains designed after real-world equivalents and described in the next. Each administrative domain follows a minimal, technology-agnostic design, delimited by a gateway router – more specifically, it contains:

- a router that functions as a gateway
- a Domain Secure Services Provider (DSSP)
- a network key generator connected to the DSSP
- at least one client

Each DSSP is a low-powered device with hardware ranging from Raspberry Pi and Android devices to x64 and RISC-V systems. The DSSP of some domains have integrated software encryptors that are cross-platform, crypto-agile packet encryptors designed to deliver high-assurance tunneling services between network domains with PQC-based multi-layer encryption and identification through PQC key pairs (see Section 5) and multi-vendor QKD support. Clients are organised in virtualized SDN network pools that combine flow rules and port policies to create a programmable network under each hardware domain. Domain components interconnect via VLAN isolation, VPN tunnelling, and identity-based segmentation under a global cloud security provider. Clients reach the domain router either directly over Wi-Fi or virtually through an SDN layer (OpenFlow 1.3 via a cloud-hosted ONOS controller, paired with a dual-mode switch supporting both SDN and non-SDN operation). The Network Address Translation (NAT) of each network domain hides their internal topology and controller-defined flow rules let the SDN switch reposition clients across domains dynamically, enabling programmatic, reconfigurable domain layouts (Figure 1). Network protection combines an open-source Network Access Control/identity manager behind a hardware firewall with MACsec and IPsec links federating external testbeds. Ultimately, all NEs are granted access to the services attached to a target cloud resting behind a cloud router, which aggregates and mediates this connectivity across the federated network of domains.

QKD nodes as key generators. The infrastructure’s versatility allows to abstract the key generator domain component to be an arbitrary device; however, one of the key contributions of the work lies with the integration of QKD nodes as key generators. Thus, we distinguish two kinds of domains, the classical or *non-quantum*, and the QKD or *quantum* domains. Classical domains adhere to classical channel communication principles. Quantum domains contain a QKD node each and are vendor-agnostic. From an operational perspective, each QKD node is associated with a specific administrative domain managed by a DSSP, which acts as a trusted proxy for inter-domain key relaying. When forwarding a key K to a neighbouring domain, the DSSP retrieves a locally generated QKD key K' from the quantum layer and computes $K \oplus K'$. The resulting value is then transmitted to the next domain, where the corresponding DSSP can recover K using the shared key material. Here, we assume the existence of inter-domain links that lack the interoperability and protection mechanisms required for seamless trusted-node operation, particularly in multi-vendor deployments, called dangling chain edges (DCEs). The chain segments between DCEs are reinforced with PQC KEMs, thus filling the chain’s non quantum-resistant gaps and yielding a chained link of arbitrary

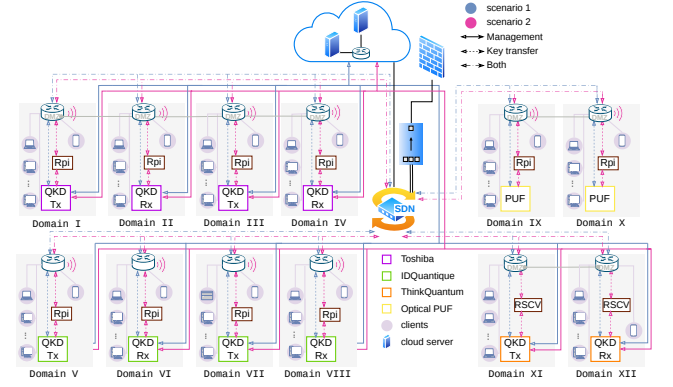


Figure 1: Detailed overview of the testbed’s architecture. Links include intradomain key transfer (dotted) and cloud management (solid). Shown are three intradomain key transfer scenarios: (1) describes usual QKD function (blue); (2) QKD keys are processed from the gateway before reaching the client (magenta); the third scenario uses a wifi link between the gateway and the client.

length. We exhibit this paradigm on a testbed of five (5) QKD pairs of different vendors, running a vendor-specific version of the BB84 protocol [5]. To safeguard DCEs, we implement an emulated equivalent of a conventional TNs via a point to point topology, provided that a MACsec tunnel has been previously setup. The tunnel can be deployed either as cloud-hosted Secure Access Service Edge (SASE) endpoints or as static on-premises endpoints. In both cases, the endpoint service embeds Identity and Access Management (IAM) and NAC through a RADIUS-based authentication and authorization interface, allowing centralized enforcement of access-control policies independently of the underlying network infrastructure. The endpoint service operates a PQC-KEM-secured post-quantum mutual TLS streaming encryptor/decryptor pair that accepts only authorized DSSPs as peers.

PUF integration. A PUF’s defining property is that it maps inputs to outputs according to physical variations introduced randomly during manufacturing, so that even devices produced identically become distinguishable from one another. This unclonable randomness can be harvested directly as key material from a key generator, rather than used solely to verify identity. Accordingly, PUFs in our architecture serve a dual role, functioning both as local, hardware-rooted key generators and as an authentication mechanism, with an abstracted PUF service layer exposing both functionalities so that an NE can request either. This service-based adoption further allows the framework to accommodate two distinct PUF types, differing in how the hardware is placed within the domain. The optical PUF is deployed as an external device, with access restricted to the DSSP alone, whereas SRAM PUFs are installed directly on the NEs, which retrieve their own response material and rely on the PUF service to confirm its validity. This placement flexibility illustrates the abstraction’s extensibility: the same service interface accommodates hardware integrated at the NE level and hardware

kept external to it, without requiring changes to how clients or DSSPs interact with the PUF layer.

Target cloud services. Authentication to services beyond the testbed is coordinated through the ESP, which extends the DSSP with local network authenticators positioned alongside the key generators, giving the DSSP the capability to handle both optical and SRAM PUF units as authenticators. To exercise this capability, the testbed has been extended with target cloud services exposing Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) functions to clients of the hardware domains; these services subscribe to the ESP as consumers of PUF-backed authentication.

4 Framework operation

In this framework, NEs distributed across domains are each provisioned with a certified identity and a PQC KEM key pair, with public keys registered on the cloud for peer-to-peer trust establishment. A NE cryptographic material request is tied to its current policy restrictions. This sequence, described below, ensures that key retrieval is gated by consistent, verifiable identity and policy checks before any QKD-produced key is released to a client.

4.1 Connecting DCEs for Multi-domain Key Distribution

Our vendor-agnostic key relay approach combines cloud-managed PQC key encapsulation and authentication with SDN functionality, reinforcing QKD across domains without distance limitations. The process unfolds in two phases: a handshake phase enforcing Zero Trust Network Access principles to ensure keys transfer only between strictly authorised parties, and a transfer phase that bypasses vendor-specific integration constraints.

Handshake phase. Domains log onto the cloud to update client policies and permissions, and clients in turn log onto their respective domain services. This login exchange authenticates each client through TLS and proof of possession of its KEM secret key, after which the domain gateway retrieves the client's authorised policy from the cloud and issues a role-based access token. Once each client holds a unique login token, the requesting peer enrolls with the initiating client's exposed service API; the initiating client stores a shared token on the cloud and expects it back from its peer as proof the peer belongs to an authenticated, accessible domain. The initiator then shares the token's identifier, and the peer resolves it via the domain services, encapsulating and presenting it back to establish mutual trust.

Transfer phase. Key delivery is handled according to the relationship between the two domains' key generators, whether these are QKD terminals or PUF-based generators, with the underlying masking and forwarding logic remaining the same regardless of the generator type. If both endpoints are QKD terminals forming a direct pair, the source DSSP masks the relay key with a locally generated QKD key and transmits the result, letting the destination DSSP recover it using shared key material. If the QKD terminals are instead connected through a TN, the relay key is masked and recovered at each hop in turn, with the trusted node re-masking it against a fresh QKD key before forwarding it onward. Where one endpoint lacks QKD infrastructure, the last hop encapsulates the

key under the destination's PQC KEM public key rather than applying another XOR mask, and the destination recovers it through decapsulation. Where endpoints are not local to QKD nodes, i.e. the key generator is not QKD-based, the latter case applies, namely, the source domain encapsulates the relay key directly under the destination's KEM public key for end-to-end delivery. Across all cases, PQC KEMs preserve quantum resistance beyond the physical reach of QKD while cloud supervision enforces controlled access, traceability, and policy compliance, even though information-theoretic security itself remains confined to the QKD segment of the path.

4.2 PUF's dual role

As a key generator, a PUF plays a role analogous to a QKD terminal's within a domain, the key material originating from the device's own physical characteristics rather than a quantum channel. As an authentication mechanism, a PUF instead produces challenge-response pairs, with the response used to identify the requesting client. In both cases, clients access the PUF service through the DSSP, mirroring the identity provision and key distribution workflow described above; this preserves the abstraction of the PUF layer and allows one or multiple PUF-equipped devices to be integrated without altering the client-facing interface. Challenge-response verification is handled by a dedicated identity provider, keeping trust orchestration secure and modular.

Authentication to target cloud services proceeds through the ESP (see Figure 2). When a client requests access to a target service, the DSSP opens a real time authentication link to the cloud supervisor, which checks the request against provisioning data held by the ESP, the PUF identity provider's records, and the target service's authorization policy. If the client is authorized, the target service receives a PQC signature token together with a nonce, while the client receives a binary message from which the matching signature can only be reconstructed once the correct nonce is applied. After the client and the service establish a mutual connection, the service transmits its nonce to the client; the client applies the nonce under the agreed algorithm to reconstruct the PQC signature and combines it with its own identity data to produce the final authentication signature. The target service, which maintains a record of signatures for each client it collaborates with, validates this signature to authenticate the device. Through this nonce-based reconstruction scheme, the ESP provides PQC-backed authentication of devices and can provision new target services on demand using the PUF units alone.

5 System Architecture and Trust Management

The presented system follows a layered architectural model consisting of an administrative plane, an SDN-orchestrated control plane, and a data plane, spanning the control, application, network, and quantum layers shown in Figure 3, the latter being treated separately due to its distinct management and operational requirements. The administrative plane constitutes the management of these layers; it defines and enforces system-wide policies, manages client permissions and possible actions, and regulates the sources of authorization material, including certificates, public key pairs, and tokens, according to user profiles. These services are domain-specific and supervised by the cloud control plane. The control

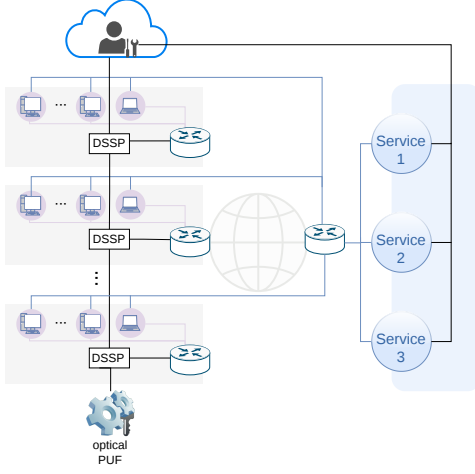


Figure 2: Relation of domains with an optical PUF, the cloud supervisor with the attached ESP and the target services.

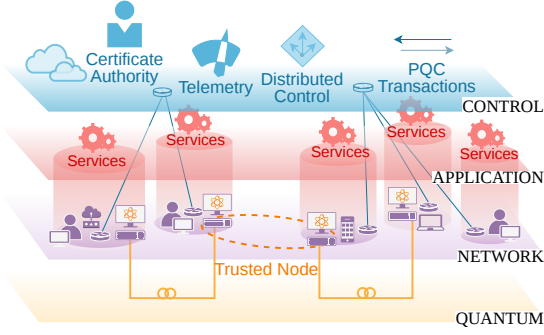


Figure 3: Overview of the proposed framework's overall organisation. The main implementation components are distributed according to the physical layout in the network.

plane leverages SDN control and automation to dynamically configure network paths, isolate traffic, and react to topology or policy changes.

5.1 Identity, Trust and Key Management

Key management provisions each NE with certificates and NTRU-based KEM key pairs, one transactional pair for cloud-based discovery, one ephemeral pair refreshed per transaction, and one for identification, with per-receiver public keys doubling as an added identity check. These provisions materialise a strict, multi-level authentication scheme combining certificates, PQC KEM key pairs, and policy alignment (domain-specific access, role-based access control). The framework employs a cloud-managed PKI with separate root and intermediate CAs for QKD nodes of different vendors versus the rest of the testbed, ensuring compatibility with distinct

chain-of-trust formats while preserving cross-chain integrity. Certificates are categorised (e.g. by role), while issuance, renewal, and revocation are managed under cloud supervision; revocation triggers dependency dismantling to reconstruct any part of the network an adversary could have accessed. Trust itself is established through cross-validation among services rather than a single centralised issuer. Gateways use mTLS, clients are initialised with post-quantum-signed certificates, and all NEs hold PQC KEM key pairs bound to their identities, with public keys stored on the cloud for peer discovery. Through the ESP, PUFs contribute nonce-bound PQC signature reconstruction in place of long-term credentials; the target service and client each hold only a partial artefact (a signature token and a nonce-dependent binary message, respectively) that must be combined correctly to authenticate. By leveraging a random AES256-encrypted payload (the client's a binary message), the PUF response and the nonce sent by the target service, the client derives the PQC signature, substituting repeated credential transmission with stateless, replay-resistant authentication at the service level. Key generators are physically isolated on a dedicated NIC and registered via device-specific identity claims (e.g. PUF or PCB features), with the DSSP invoking a generator-specific driver to handle key requests accordingly. This ZTP-driven, claim-based provisioning scheme keeps key retrieval fully agnostic to the underlying generator hardware, enabling secure integration of any device type.

5.2 Vendor-agnostic QKD Management

A significant portion of effort addressed the seamless incorporation of the QKD pairs. QKD management is performed from the cloud and is designed to accommodate the requirements of the devices in our testbed, while remaining readily extensible to support additional hardware. This module is meant to efficiently provide access to cryptographic material while maintaining smooth operation and communication with the domain, as commercial QKD devices frequently depend on rigid configuration requirements, limiting seamless integration in large-scale, multi-vendor environments. In our implementation, we found misalignment on four (4) levels, including administration or management, authentication mechanisms, SDN support and key retrieval interfaces.

5.3 Orchestration and Telemetry

The orchestration layer manages coordination and automation of network, control, and quantum resources across domains. It provides consistent configuration, deployment, but also integrates with the SDN controller to allow dynamic configuration, monitoring, and reconfiguration of network paths in response to topology changes or policy decisions. In the context of this work, orchestration plays a central role in the controlled bridging of high-level components with low-level system elements. A key function of the orchestration layer is the support for automated scenario building, whereby network topologies, domain relationships, and service dependencies can be instantiated programmatically. This includes the definition of participating network elements, inter-domain links, and associated control policies. The continuous stream of detailed logs and audit produces a voluminous set of output, balanced by the telemetry component. Telemetry has been tuned to be device-oriented and

Platform	Role	Specifications
Poweredge R730	cloud server	32 cores, 32GB, Ubuntu server 24.04, PCIe 3.0
Laptop	client	i7-13700H, 20 cores, 16GB, Ubuntu 25.04, PCIe 4.0
Raspberry Pi 5	DSSP	2GB, 4-core Aarch64, kernel SMP
Raspberry Pi 4	DSSP	Raspbian Lite, 32GB, heatsink (no fan), 6.12 SMP PREEMPT
RISCV64	DSSP	SiFive P550 Premier, ARM RISCV64, 32GB, SMP PREEMPT_DYN

Table 1: Devices used in our testbed with their specifications and role.

Platform	Encryption	Decryption
RISCV64 (full desktop)	2.5 ms	24 ms
Raspberry Pi 4 (full desktop)	2.5 - 4 ms	6.5 ms
Raspberry Pi 5 (no desktop)	2.5 ms	6.5 ms

Table 2: Times for encryption and decryption of the encapsulated packet travelling between domains.

Platform	1 KEM pair	4 KEM pairs
Laptop	37.58	125.26
Cloud server (2 cores)	71	280.31
Cloud server (10 cores)	71	280.31

Table 3: Measurements regarding the creation of key pairs on each device of Table 1. The KEM used is NTRU761. The results are reported in milliseconds.

to provide a clear image of the network’s status, enabling observability and the rapid identification of problematic segments. To this end, telemetry data are collected and aggregated across domains, allowing both localized and system-wide conditions to be assessed in a consistent manner. NEs are granted with some control over their relevant logging allowing them to enable, disable, or trigger logging operations manually.

6 Experimental Results

We conducted experiments on a testbed of ten (10) domains containing QKD nodes from three vendors, alongside two (2) domains without QKD nodes. Each domain includes a gateway router, a low-power DSSP device, and client nodes (Table 1), while an aggregation router enables inter-domain and cloud connectivity via an SDN-enabled data plane. QKD communication relies on ETSI 014 [8].

The implementation avoids dependencies (e.g. the OQS project [16]), relying instead on portable standardized algorithm releases for reproducibility, and is deployed as a hidden, non-discoverable directory-service layer alongside existing directory models. Cryptographic operations run through a lightweight, custom application-layer library with minimal kernel dependencies, keeping the software portable and easy to integrate with existing applications.

RSA-4096 costs dominate certificate generation overall. On the laptop, building the full CA-ICA tree (18 certificates) takes 412 ms, while initialising the QKD infrastructure requires roughly 1227 ms,

Platform	CA - ICA (18 crts)	QKD (16 crts)
Laptop	411.82	1227.35
Cloud server (2 cores)	4377.59	16888.82
Cloud server (10 cores)	4377.59	13443.88

Table 4: Measurements regarding the creation of certificates on each device of Table 1. A part of the listed certificates were produced with ECDSA P-384 and the rest with RSA 4096. The results are reported in milliseconds.

of which only ~ 27 ms stems from ECDSA P-384 and the remaining ~ 1200 ms from RSA. This initialisation cost rises to ~ 13.4 – 16.9 s in cloud environments, again driven primarily by RSA generation, with additional CPU cores yielding little improvement. Tables 3,4 reports the measured certificate and KEM generation overhead across all platforms.

Taken together, these results indicate that SDN control and service orchestration add only modest, manageable overhead even on constrained hardware. The principal bottlenecks instead lie in QKD key retrieval and infrastructure initialisation, where vendor-specific implementations trade higher latency for greater robustness and stronger authentication support. Classical certificate generation proves highly resource-sensitive, while PQC operations perform consistently regardless of platform.

7 Conclusions

We have presented an infrastructure that supplies quantum-secure communication among network elements and extends to cloud services through PUF-based authentication. Building this as a set of services, synced with cloud administration for secure, per-user, up-to-date policies, keeps the system non-intrusive, crypto-agile, and adaptable to any domain topology. PUF-based authentication best illustrates this design. Fully decoupled from the key-provider services (QKD, or PQC KEMs emulating it beyond distance limits), it onboards as a new trust mechanism without touching the client-facing interface or the core domain logic. This matters because PQC adaptation for devices participating in a PKI otherwise stays low-level and manufacturer-dependent, tied to whichever CAs a vendor has built out. Authentication rooted in the device’s own PUF sidesteps that dependency entirely.

Realising this still demands considerable management work across heterogeneous hardware and operating systems, met through small, native, distributed modules that speak to each device on its own terms. That same native design accelerates PQC implementation, keeping it portable, reliable, and fast, with markedly lower and more consistent overhead than classical algorithms like RSA across the platforms tested.

8 Acknowledgements

This research was partially funded by the European Union through the projects ALLEGRO (Grant Agreement No. 101092766) and Hel-lasQCI (Grant Agreement No. 101091504).

References

- [1] Marialena Akriotou, Theodoros Bartsokas, Christos Veinidis, and Dimitris Syvridis. 2025. Optimal performance of simple low-cost optical physical unclonable functions resilient to machine learning attacks. *Scientific Reports* 15, 1 (17 Nov 2025), 40079. doi:10.1038/s41598-025-23840-z
- [2] Raed Alhamarneh and Manmeet Mahinderjit Singh. 2024. Strengthening Internet of Things Security: Surveying Physical Unclonable Functions for Authentication, Communication Protocols, Challenges, and Applications. *Applied Sciences* 14 (02 2024), 1700. doi:10.3390/app14051700
- [3] Asier Atutxa, Ane Sanz, Eire Salegi, Maider Huarte, Jasone Astorga, and Eduardo Jacob. 2025. Authentication of the QKD classical channel through Post-Quantum Cryptography in a multi-site 5G/6G quantum-safe communication network. In *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. IEEE, Nara, Japan, 648–654. doi:10.1109/QCNC64685.2025.00108
- [4] David Barral, Aitor Brazaola-Vicario, Diego Cifrián, Natalia Costas, Gonzalo Blázquez, Ana Fernández-Vilas, Iago F. Llovo, Pedro Otero-García, Pablo P. Rejo, Alejandra Ruiz, Juan Villasuso, and Manuel Fernández-Veiga. 2026. Interconnecting Regional QKD Networks: Hybrid Key Delivery Across Quantum Domains. arXiv:2604.20376 [cs.NI]. doi:10.48550/arXiv:2604.20376
- [5] Charles H Bennett and Gilles Brassard. 1984. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175. Bangalore, India.
- [6] Vinay Chamola, Alireza Jolfaei, Vaibhav Chanana, Prakhari Parashari, and Vikas Hassija. 2021. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. *Computer Communications* 176 (Aug. 2021), 99–118. doi:10.1016/j.comcom.2021.05.019
- [7] Emir Dervisevic, Amina Tankovic, Ehsan Fazel, Ramana Kompella, Peppino Fazio, Miroslav Voznak, and Miralem Mehic. 2025. Quantum Key Distribution Networks - Key Management: A Survey. *Comput. Surveys* 57, 10 (Oct. 2025), 1–36. doi:10.1145/3730575
- [8] European Telecommunications Standards Institute. 2019. *Quantum Key Distribution (QKD): Protocol and Data Format of REST-based Key Delivery API*. Technical Report. European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France. Defines a protocol and data format for REST-based key delivery in QKD networks. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf
- [9] Juan Antonio Vieira Giestinhas and T. Spiller. 2025. On Post-Quantum Cryptography Authentication for Quantum Key Distribution. *ArXiv abs/2507.21325* (2025). doi:10.48550/arxiv.2507.21325
- [10] Sergejs Kozlovics, Krisjanis Petrucena, Davis Larins, and Juris Viksna. 2023. Quantum Key Distribution as a Service and Its Injection into TLS. In *Information Security Practice and Experience*, Weizhi Meng, Zheng Yan, and Vincenzo Piuri (Eds.). Vol. 14341. Springer Nature Singapore, Singapore, 527–545. Series Title: Lecture Notes in Computer Science. doi:10.1007/978-981-99-7032-2_31
- [11] Rubén B. Méndez, Hans H. Brunner, Juan P. Brito, Hamid Taramit, Chi-Hang Fred Fung, Antonio Pastor, Rafael Cantó, Jesús Folgueira, Diego R. López, Momtchil Peev, and Vicente Martín. 2026. Switching Coordinator: An SDN Application for Flexible QKD Networks. *Entropy* 28, 2 (Feb. 2026), 219. doi:10.3390/e28020219
- [12] V. Martín, J. P. Brito, L. Ortiz, R. B. Méndez, J. S. Buruaga, R. J. Vicente, A. Sebastián-Lombráña, D. Rincón, F. Pérez, C. Sánchez, M. Peev, H. H. Brunner, F. Fung, A. Poppe, F. Fröwis, A. J. Shields, R. I. Woodward, H. Griesser, S. Roehrich, F. De La Iglesia, C. Abellán, M. Hentschel, J. M. Rivas-Moscoso, A. Pastor-Perales, J. Folgueira, and D. López. 2024. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Information* 10, 1 (Sept. 2024), 80. doi:10.1038/s41534-024-00873-2
- [13] Ruben B. Mendez, Jaime S. Buruaga, Rafael J. Vicente, Luis Mengual, Antonio Pastor, Alejandro Muñoz, Juan Morales, Rafael Canto, Jesus Folgueira, Diego R. Lopez, Vicente Martin, and Juan P. Brito. 2024. SDN-Based Hybrid Quantum-Safe Domain Intercommunication Within MadQCI. In *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. IEEE, Kanazawa, Japan, 168–175. doi:10.1109/QCNC62729.2024.00034
- [14] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. 2002. Physical One-Way Functions. *Science* 297, 5589 (2002), 2026–2030. arXiv:<https://www.science.org/doi/pdf/10.1126/science.1074376> doi:10.1126/science.1074376
- [15] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. 2010. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security* 18, 1 (Jan. 2010), 61–87. doi:10.3233/JCS-2010-0373
- [16] Douglas Stebila and Michele Mosca. 2017. Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project. In *Selected Areas in Cryptography – SAC 2016 (Lecture Notes in Computer Science, Vol. 10532)*. Springer, 14–37. doi:10.1007/978-3-319-69453-5_2
- [17] Antonia Tsili, Konstantinos Kordolaimis, Konstantinos Krilakis, and Dimitris Syvridis. 2025. A Scalable Framework for Post-Quantum Authentication in Public Key Infrastructures. In *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. 279–286. doi:10.1109/QCNC64685.2025.00052
- [18] Chaokun Wang, Sijiang Xie, Yalong Yan, and H. Zhao. 2026. Hash-Based Signature Authentication for Scalable and Security-Consistent QKD Post-Processing. *Computers, Materials & Continua* (2026). doi:10.32604/cmc.2026.077994
- [19] Liu-Jun Wang, Kaiyi Zhang, Jia-Yong Wang, Jie Cheng, Yong-Hua Yang, Shi-Biao Tang, Di Yan, Yan-Lin Tang, Z. Liu, Yu Yu, Qiang Zhang, and Jian-Wei Pan. 2020. Experimental authentication of quantum key distribution with post-quantum cryptography. *npj Quantum Information* 7 (2020). doi:10.1038/s41534-021-00400-7
- [20] Qingping Wang, Xiaosong Yu, Qingcheng Zhu, Yongli Zhao, and Jie Zhang. 2021. Quantum key pool construction and key distribution scheme in multi-domain QKD optical networks (QKD-ON). In *4th Optics Young Scientist Summit (OYSS 2020)*, Chaoyang Lu, Yangjian Cai, Feng Chen, and Zhaoxue Li (Eds.). SPIE, Ningbo, China, 63. doi:10.1117/12.2591316
- [21] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. 2020. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* 92 (May 2020), 025002. Issue 2. doi:10.1103/RevModPhys.92.025002
- [22] Yong-Hua Yang, Peiya Li, Shi-Zhao Ma, Xiaoming Qian, Kaiyi Zhang, Liu-Jun Wang, Wanlin Zhang, Fei Zhou, Shi-Biao Tang, Jia-Yong Wang, Yu Yu, Qiang Zhang, and Jian-Wei Pan. 2021. All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Optics express* 29 16 (2021), 25859–25867. doi:10.1364/oe.432944
- [23] Qingcheng Zhu, Xiaosong Yu, Yongli Zhao, Avishek Nag, and Jie Zhang. 2024. QKD Key Provisioning With Multi-Level Pool Slicing for End-to-End Security Services in Optical Networks. *IEEE Transactions on Network Science and Engineering* 11, 2 (March 2024), 2153–2169. doi:10.1109/TNSE.2023.3338734