# On the Road to Scalable Quantum Communications: The Benefits of Network Programmability

Asier Atutxa, EHU/RedIRIS

David Franco, EHU/RedIRIS

Participants in GÉANT GN5-2 WP6 Task 1 - RARE

Infoshare: Community-Built Quantum Communication Tools, Virtually hosted

03 December 2025

# Agenda

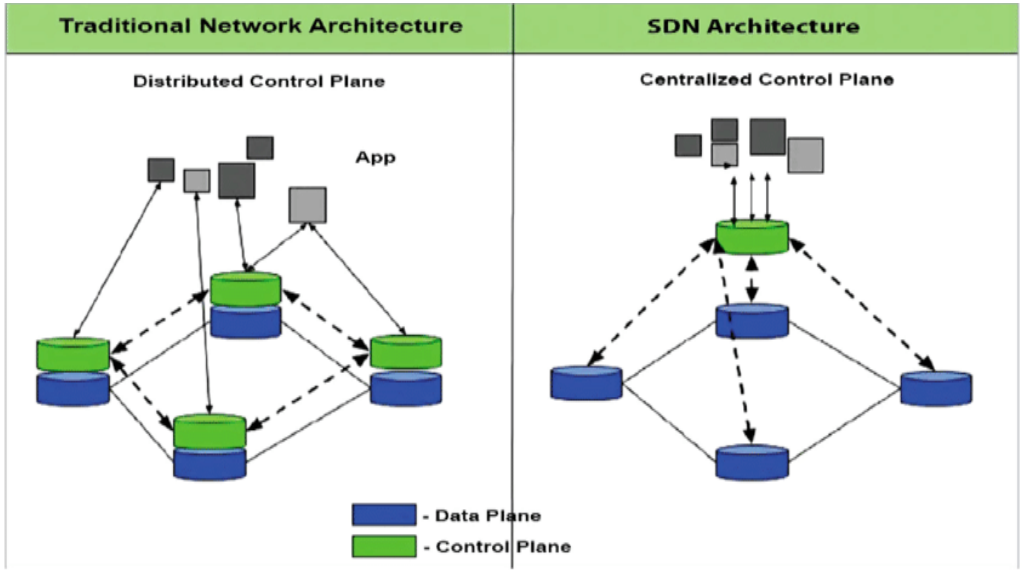
- Challenges of quantum networks
- Control plane programmability and QKD
- Data plane programmability and QKD
- Conclusions

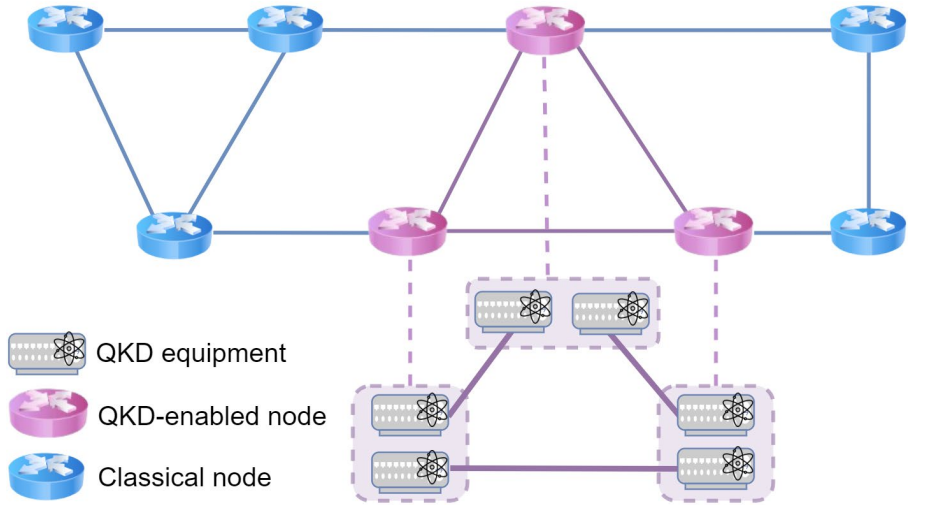
# Challenges of quantum networks

- Similar challenges of traditional networks
  - Key distribution and management
  - Resource constraints and scalability
  - Multi-domain and heterogeneous networks
- Classical SDN concepts applied to quantum
  - Distributed routing protocols
  - Centralized approaches
  - High-level orchestration
  - Implementation of interoperability protocols
- Additional challenges

Range → Trust → Cost → Key rate

Fig. 1. Traditional network vs SDN network [1]

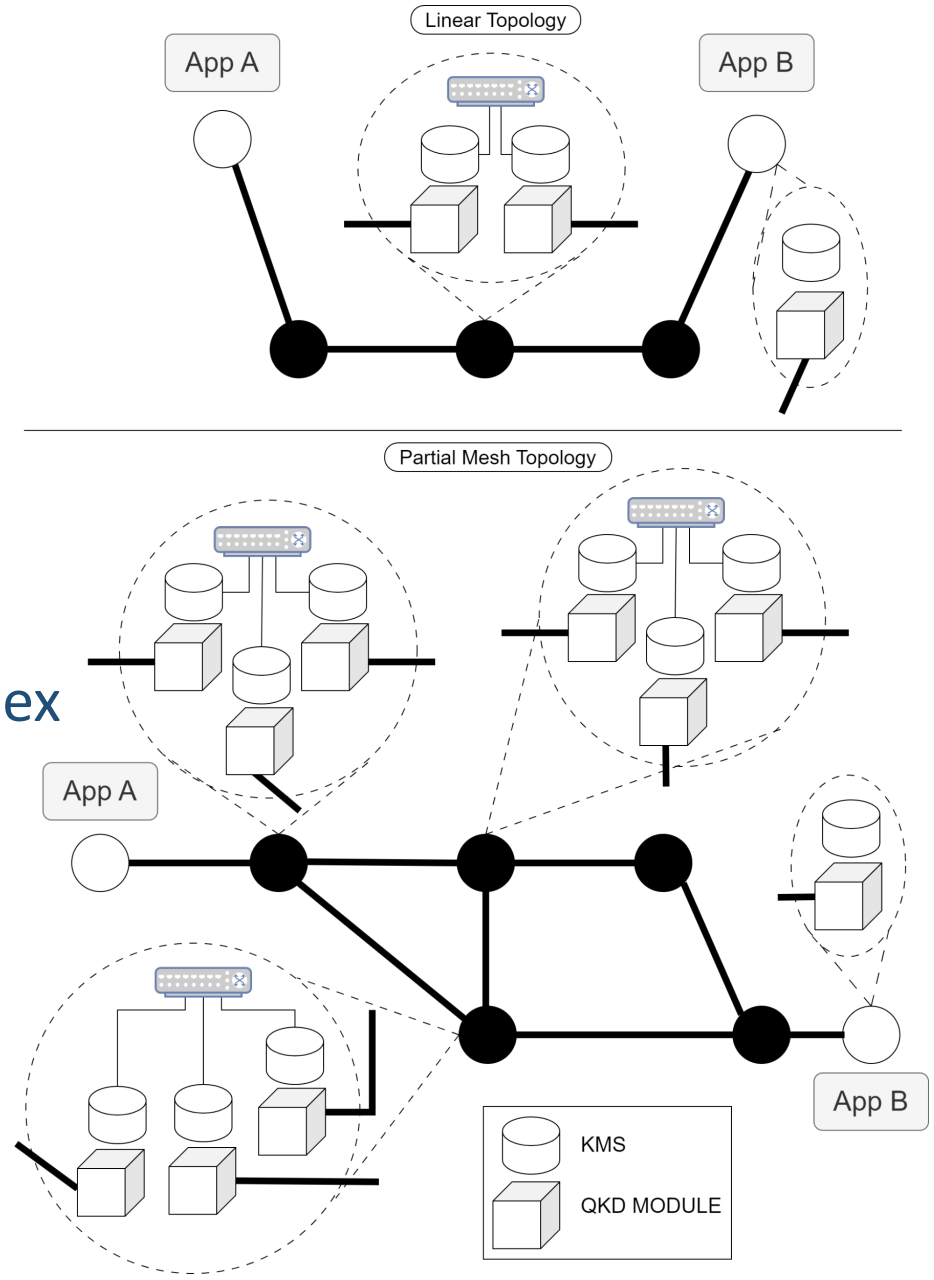



[1] New Architecture Design of Cloud Computing Using Software Defined Networking and Network Function Virtualization Technology - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Traditional-network-vs-SDN-network-10_fig1_336989337 [accessed 2 Dec 2025]

# Challenges of quantum networks

- Ideal scenario: full QKD-enabled nodes
- Real scenario: transition limited by constraints
  - Heterogeneous networks
    - QKD-enabled nodes
    - PQC-enabled classical nodes
- End-to-end (E2E) security establishment complex
  - Trusted relay → Solves QKD key extension
  - Question: control and path establishment?
    - Linear topologies → Straightforward
    - Partial mesh topologies → Dynamic



# Challenges of quantum networks

- Network programmability: excellent tool to solve the challenges
- Different approaches:

1

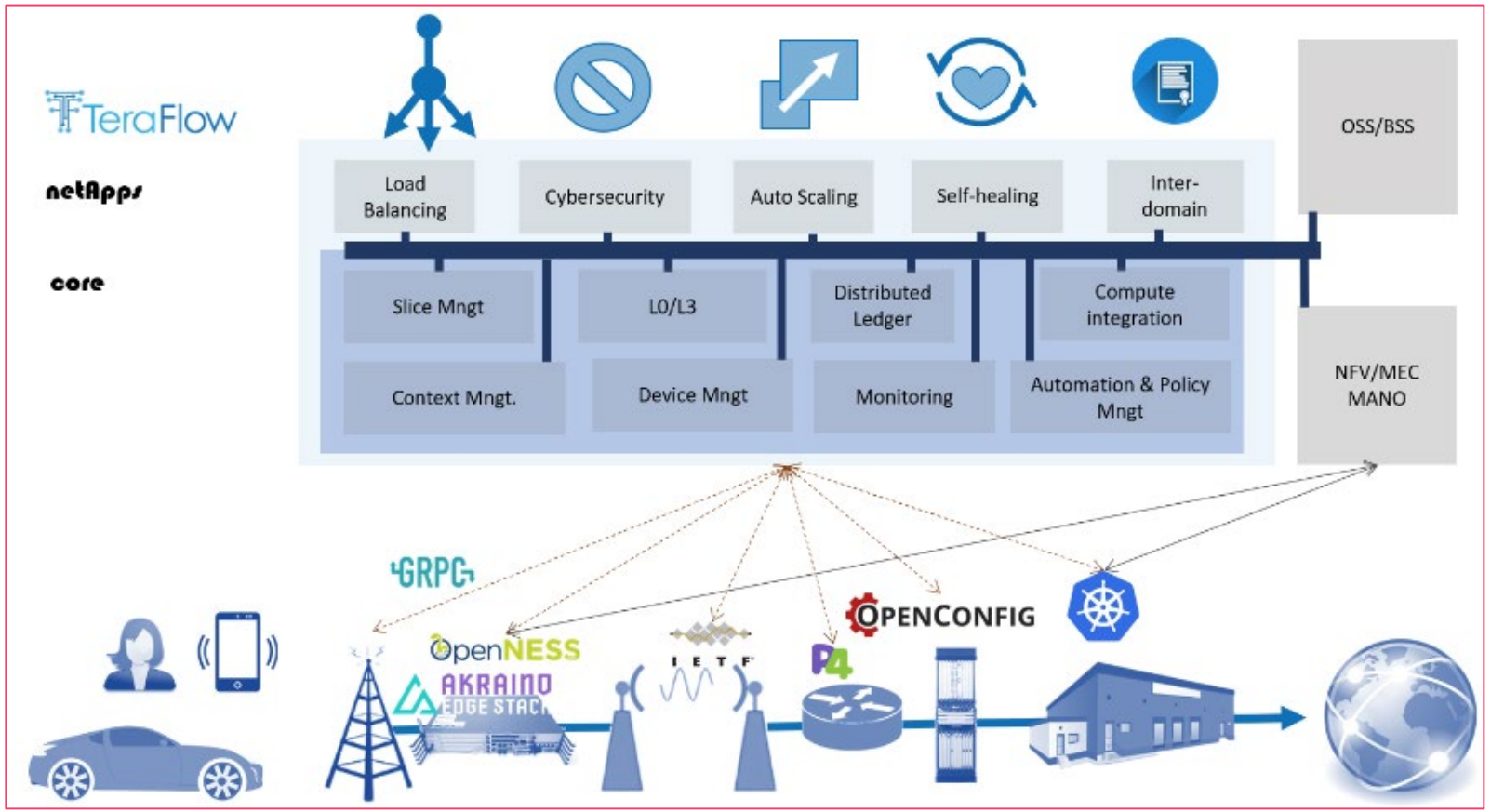
**Control plane**

2

**Data plane**

# Control Plane programmability and QKD

- Current trends
  - **TeraFlowSDN**
    - Architecture

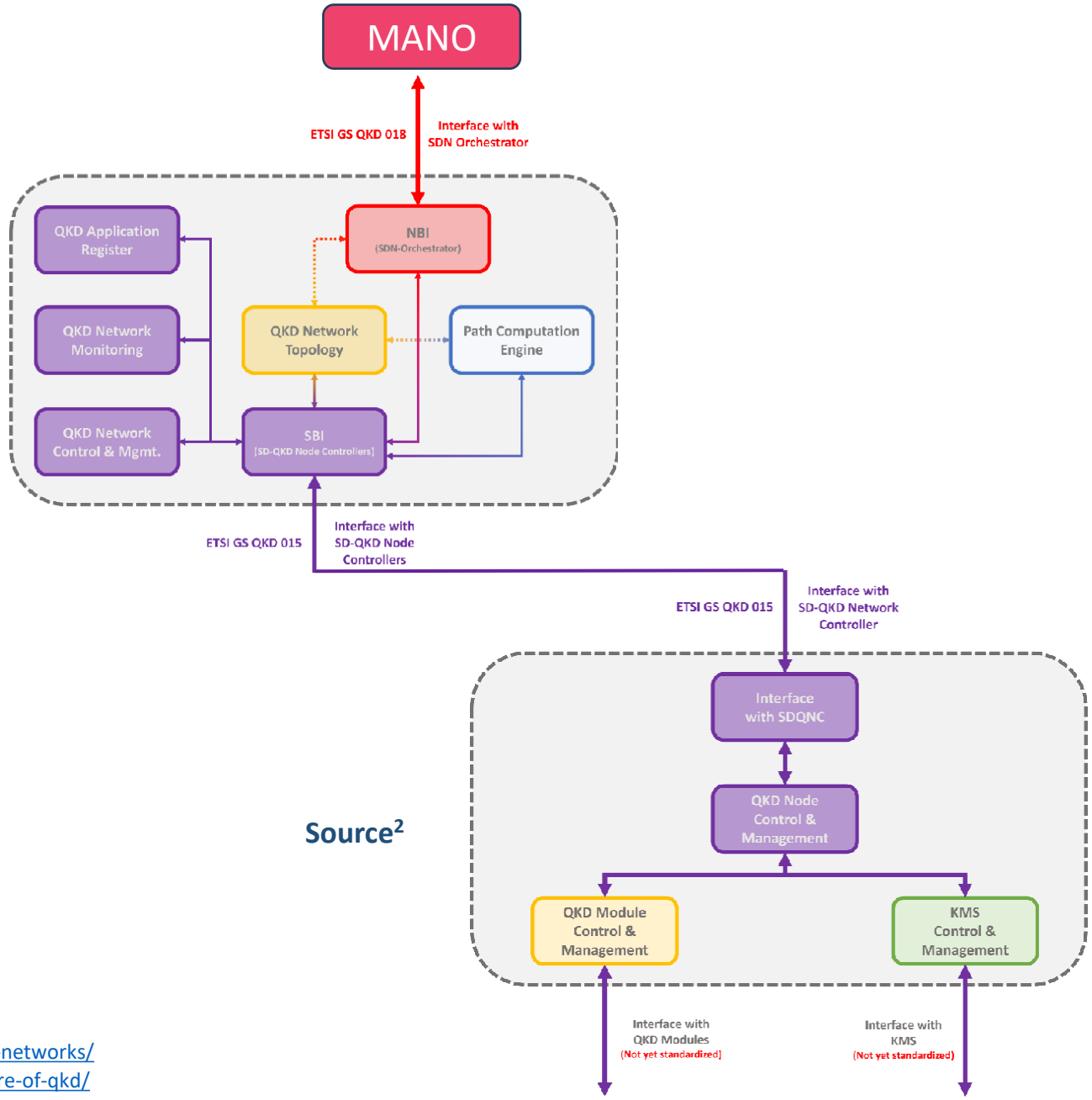



Source[2]

[1] https://doi.org/10.1109/EuCNC/6GSummit51104.2021.9482469

# Control Plane programmability and QKD

- Current trends
  - **TeraFlowSDN**
    - Support for QKD systems: 6G-OPENSEC-KEYS project[1]
      - NBI: ETSI GS QKD 018
        - Interface to orchestrator
      - SBI: ETSI GS QKD 015
        - Interface to QKD node

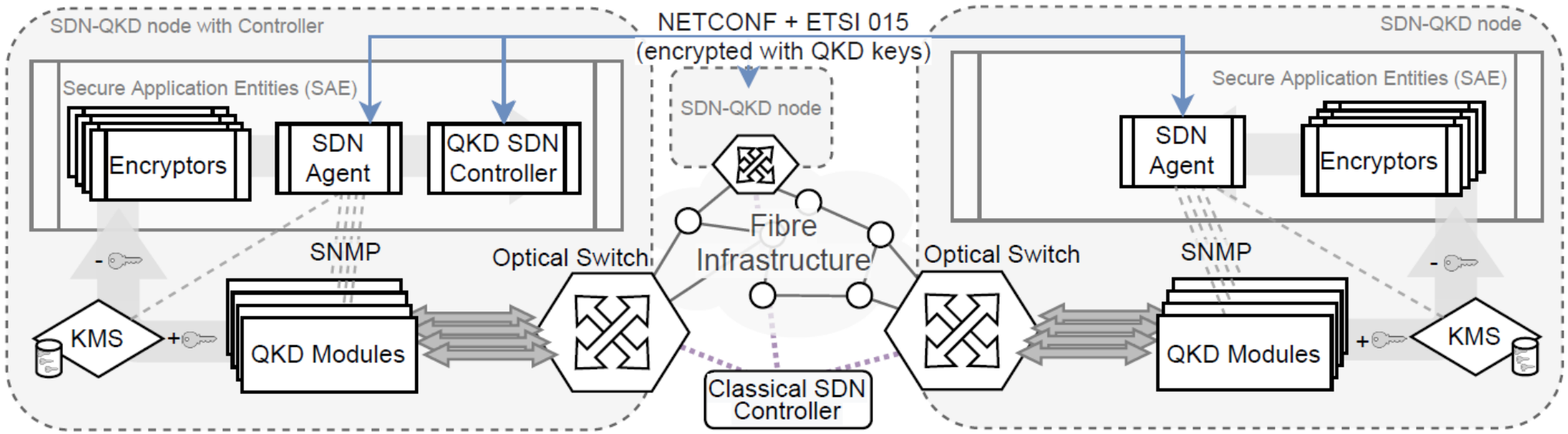



Source[2]

[1] https://www.cttc.cat/project/quantum-key-distribution-for-security-in-open-and-disaggregated-6g-networks/
[2] https://optaresolutions.com/en/open-quantum-networks-with-teraflowsdn-the-interoperable-future-of-qkd/

# Control Plane programmability and QKD

- Current trends
  - QKD-secured SDN controller[1]
    - Developed by Toshiba
    - An SDN controller for QKD nodes that uses QKD keys to secure the controller-to-QKD node interface

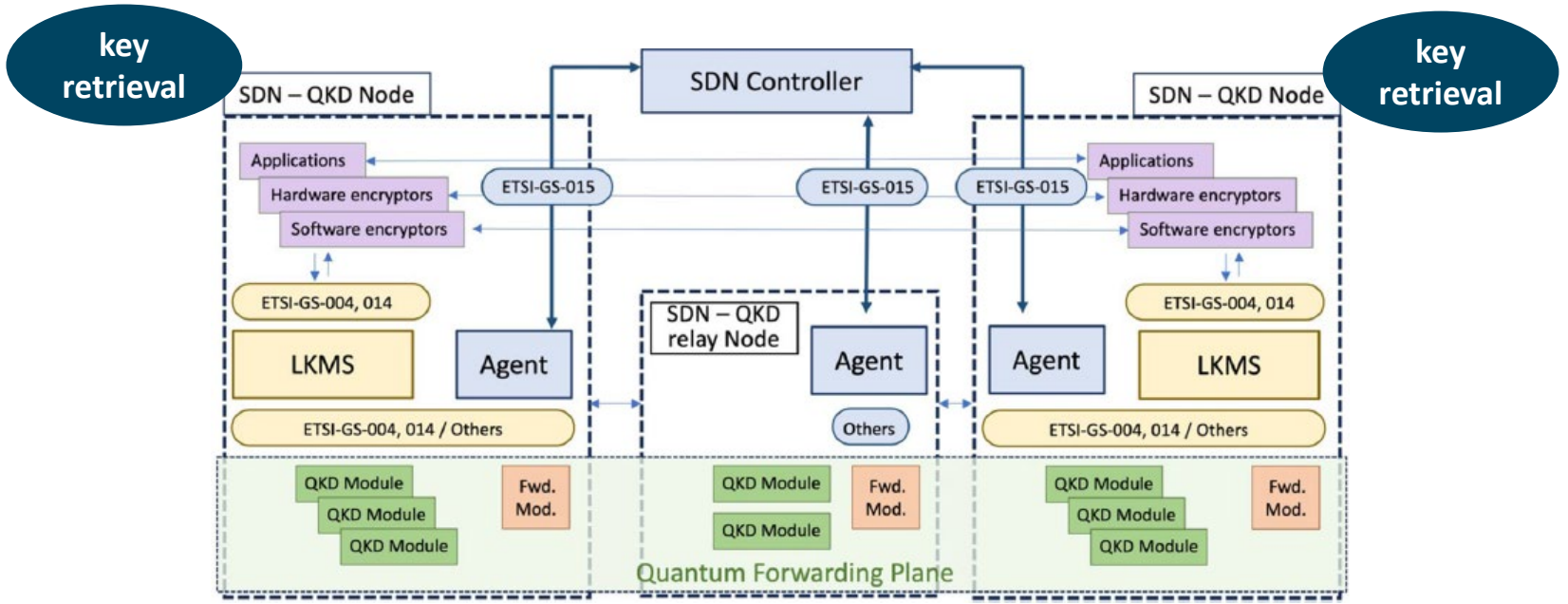



Source[1]

[1] https://arxiv.org/abs/2305.12893

# Control Plane programmability and QKD

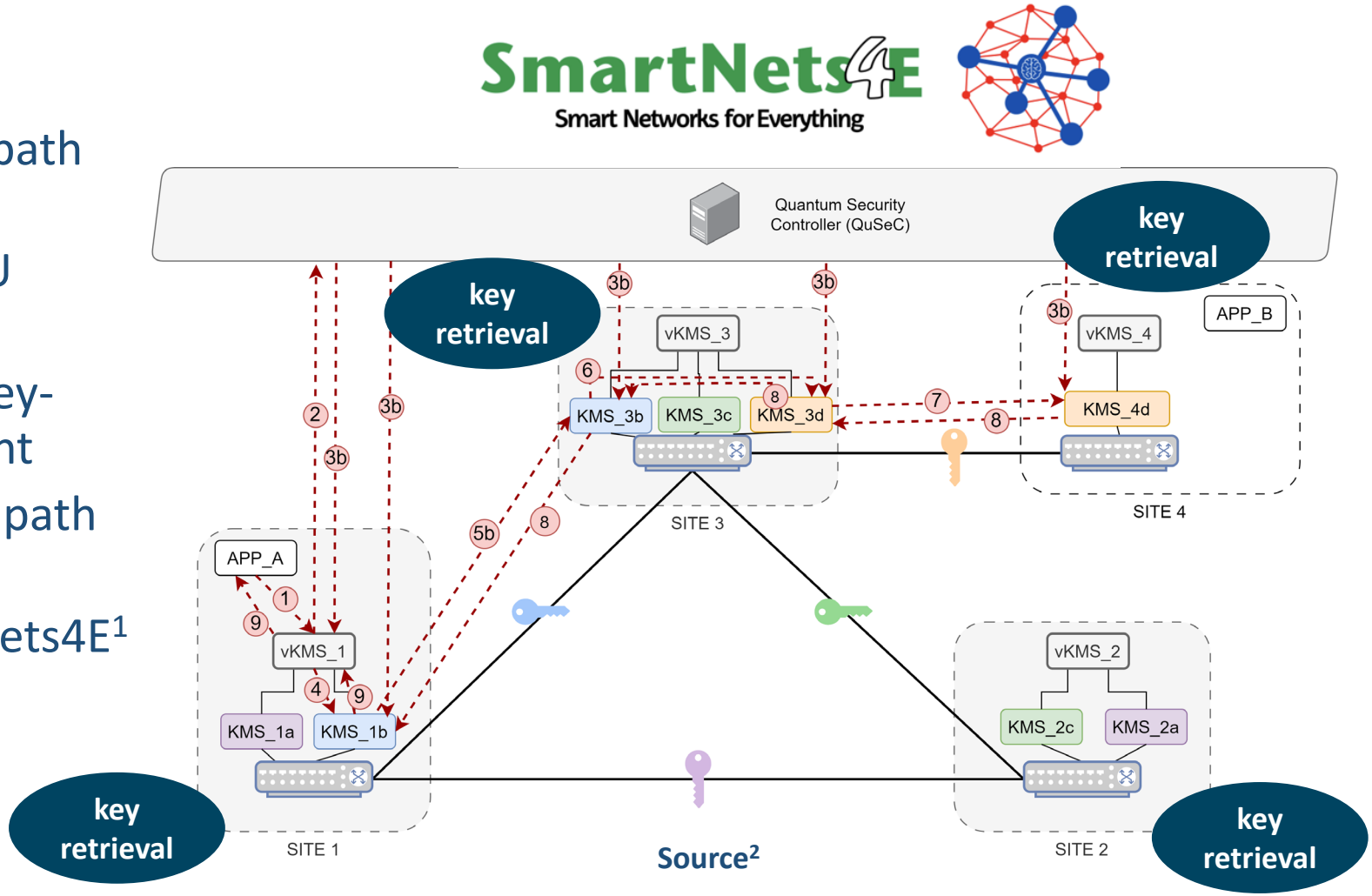
- Current trends
  - **MadQCI**
    - The controller creates the logical and physical connections necessary for sharing a key end-to-end
    - Intermediate nodes do not support key retrieval




[1] https://www.nature.com/articles/s41534-024-00873-2

# Control Plane programmability and QKD

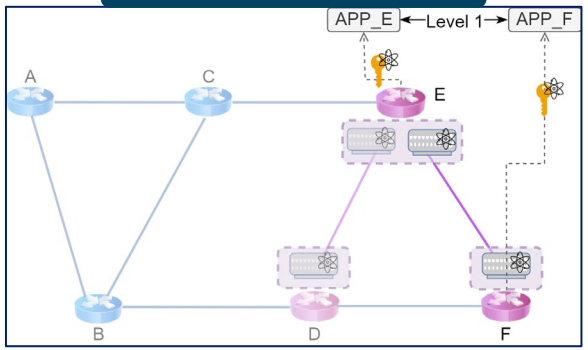
- Current trends
  - **QuSeC**: dynamic key-relay path establishment
    - Developed by UPV/EHU
    - Centralised quantum controller to manage key-relay path establishment
    - Find the best key-relay path between two sites
    - Integrated into SmartNets4E[1] (shared with GP4L)



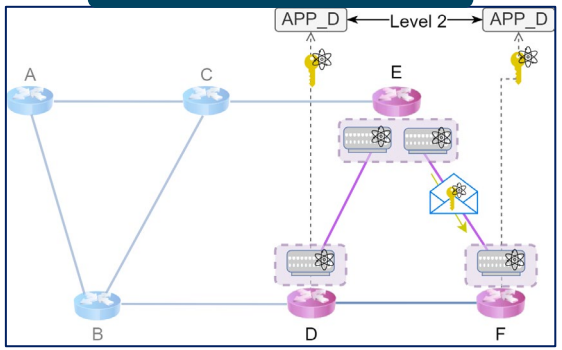

[1] https://i2t.ehu.eus/en/resources/8/smartnets4e
[2] https://arxiv.org/abs/2509.09453

# Control Plane programmability and QKD

Level 1: direct QN-to-QN

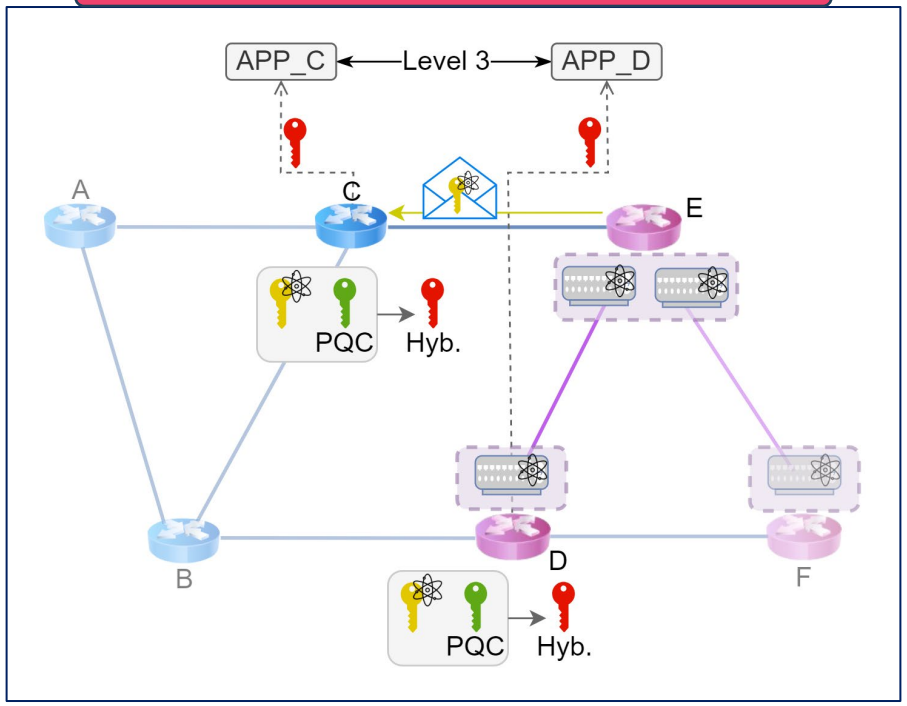



Level 2: multi-hop QN-to-QN

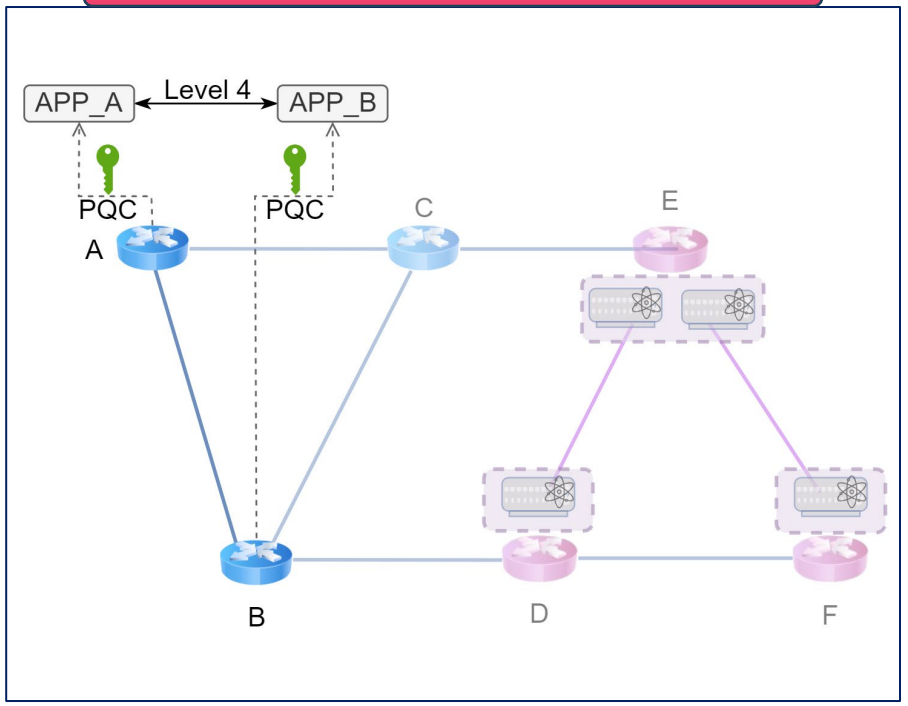



- Potential research lines
  - **QuSeC and PQC**: security levels[1]
    - Extending quantum-level security to non-QKD nodes

Level 3: Classical Node to Quantum Node




Level 4: Classical Node to Classical Node

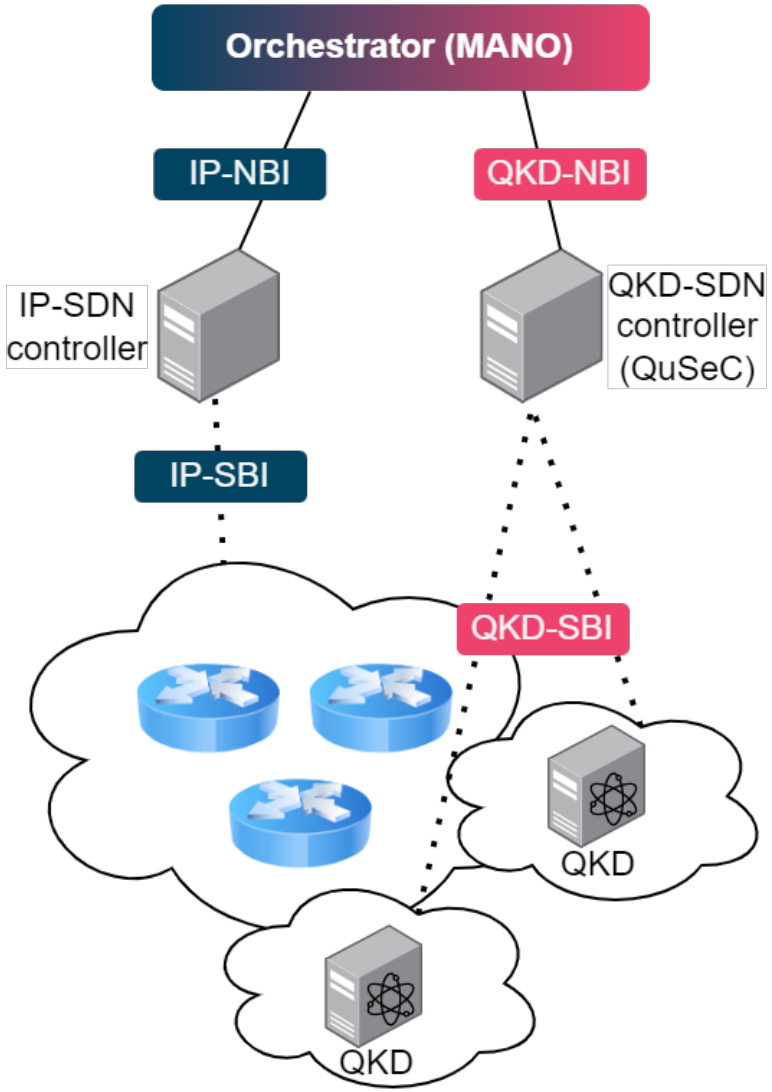



**Source**[1]

[1] https://arxiv.org/abs/2511.22416

# Control Plane programmability and QKD

- Potential research lines
  - Orchestration of IP and QKD resources
    - Single point of M&O for IP and QKD domains
    - Interfaces
      - IP-NBI: Controller-dependent (REST, etc.)
      - QKD-NBI: ETSI GS QKD 018
      - IP-SBI: NETCONF, OpenFlow, P4Runtime, etc.
      - QKD-SBI: ETSI GS QKD 015
    - Could be extended to multi-domain scenarios



# Data Plane programmability and QKD

- Current trends

**Quantum channel integration and multiplexing in classical channels/networks**

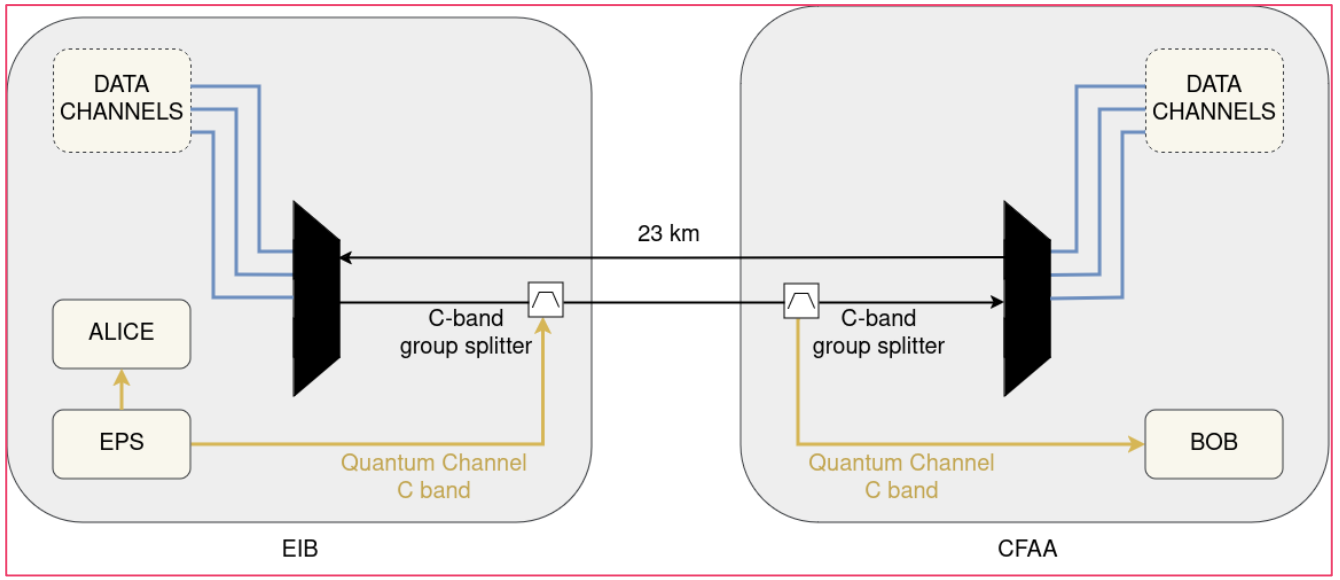
- Coexistence approaches (i.e. co-propagation)

**Multi-layer cryptographic integration in the data plane**

- Physical level (optical networks)
- Link and network layers (several protocols, IPsec, MACsec…)
- High-level layers (application-level encryption)

# Data Plane programmability and QKD

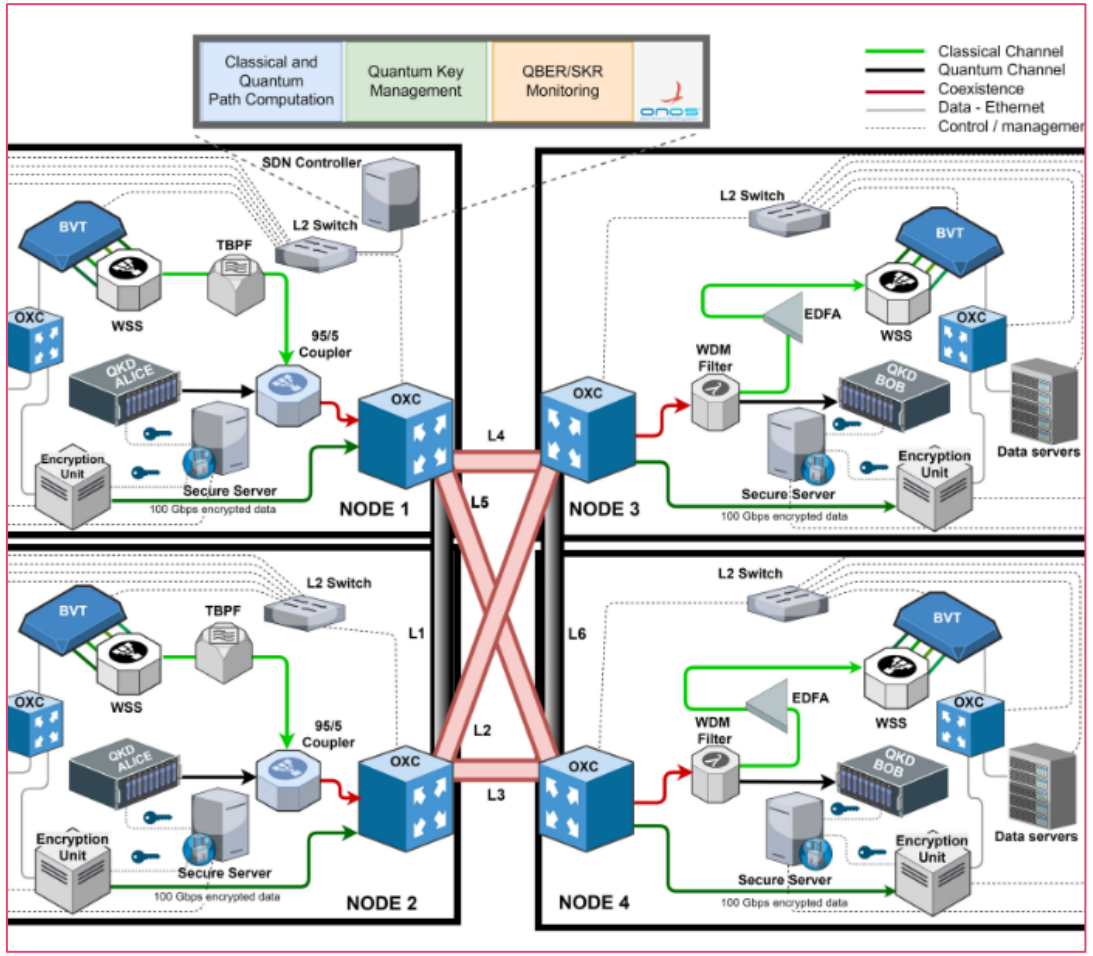
- Current trends
  - **Optical network integration**: Typically integrated into Dense Wavelength Division Multiplexing (DWDM)
    - Objective: Coexistence of classical and quantum channels in the same fibers
    - Removes the requirement of dark fibers




A. Sanz, A. Atutxa, D. Franco, J. Astorga and E. Jacob, "Adapting communication networks to the quantum safe era: lessons learned in the coexistence of polarization-entangled QKD and classical channels," 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Nara, Japan, 2025, pp. 110-116, doi: 10.1109/QCNC64685.2025.00025

# Data Plane programmability and QKD

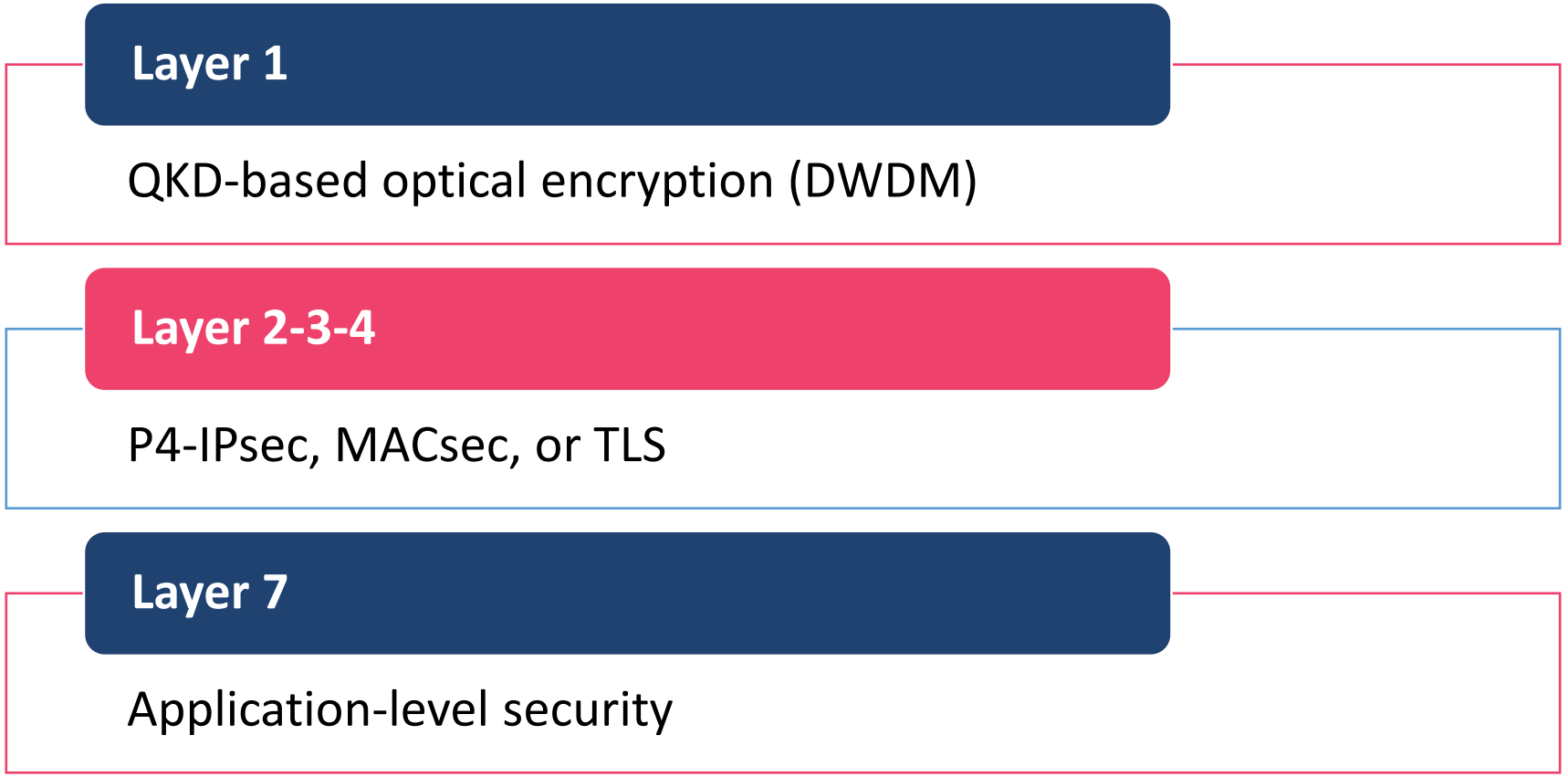
- Current trends
  - Programmability in quantum optical networks:
    - Optical controllers can configure parameters and dynamically allocate wavelengths
  - Result:
    - Dynamically move a QKD channel away from a heavily loaded classical wavelength
    - Change from single-fiber bidirectional to dual-fiber operation
    - Reallocate quantum capacity to different trusted nodes
  - Example Alia *et al.*: A controllable q-ROADM is used to enable classical data channels and QKD signal routing and switching functionality.




O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati and D. Simeonidou, "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks," in Journal of Lightwave Technology, vol. 40, no. 17, pp. 5816-5824, 1 Sept.1, 2022, doi: 10.1109/JLT.2022.3183962

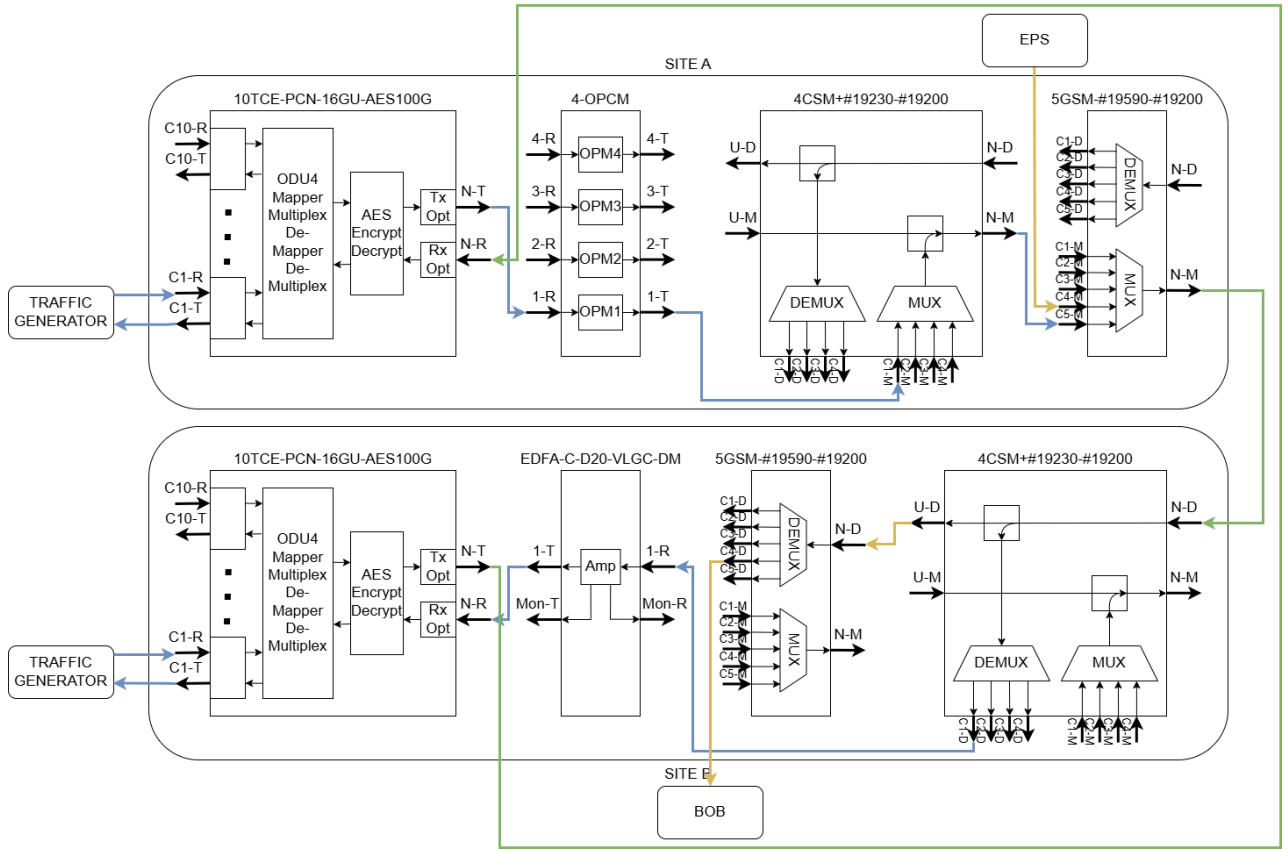
# Data Plane programmability and QKD

- Current trends
  - Multi-layer Cryptographic Approach



# Data Plane programmability and QKD

- Current trends
  - Layer-1 Optical Encryption: Quantum-safe 400G at physical layer using DWDM
    - Transparent Encryption: Line-rate at OTN/optical level
    - QKD Integration: Layer-1 encryption with QKD key supply




A. Sanz, A. Atutxa, D. Franco, J. Astorga and E. Jacob, "Adapting communication networks to the quantum safe era: lessons learned in the coexistence of polarization-entangled QKD and classical channels," 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Nara, Japan, 2025, pp. 110-116, doi: 10.1109/QCNC64685.2025.00025

# Data Plane programmability and QKD

- Current trends
  - Higher layers: programmable data planes implement efficient symmetric encryption with these keys at Layers 2 – 4
  - Heterogeneous networks make use of protocols depending on the requirements and network segments (i.e. 5G networks).

**QKD-backed IPsec**

- PSK-based IKE auth. and ESP tunnelling

**PQC/QKD-based TLS**

- PSK only (authentication and encryption)
- Asymmetric authentication (public key crypto) and symmetric encryption

**Hybrid combinations**

- Multi-technology environments (quantum and non-quantum nodes)

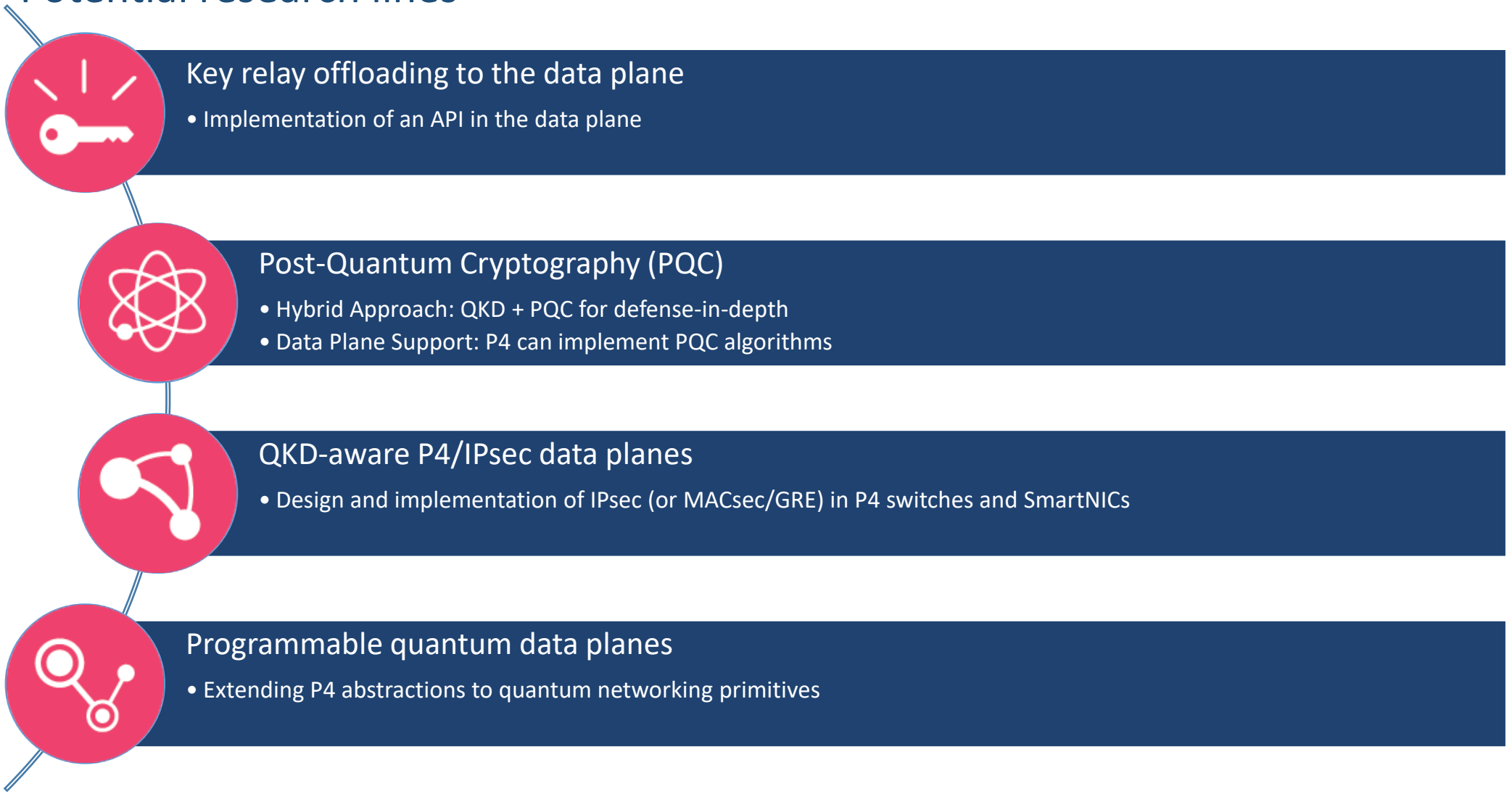
# Data Plane programmability and QKD

- Current trends
  - Quantum Internet
    - Beyond QKD key-relay
    - E2E exchange of qbits (entanglement)
    - Layered communication architecture (like in classical networks)
  - **QuIP[1]**
    - A framework to prototype Quantum Internet protocols
    - P4-like abstraction to describe the operation of a “quantum plane”

[1] W. Kozlowski, F. A. Kuipers, R. Smets and B. Turkovic, "QuIP: A P4 Quantum Internet Protocol Prototyping Framework," in IEEE Journal on Selected Areas in Communications, vol. 42, no. 7, pp. 1936-1949, July 2024, doi: 10.1109/JSAC.2024.3380096., https://ieeexplore.ieee.org/abstract/document/10482892

# Data Plane programmability and QKD

- Potential research lines



# Conclusions

- Benefits of network programmability in quantum networks

**1** **Real-time rerouting in case of quantum link failures**

**2** **Dynamic configuration of key-relay paths**

**3** **Orchestration of both quantum and classical resources**

- QKD key retrieval and management from KMSs
- Communication resource management to establish E2E communication

**4** **Data plane processing to carry out quantum-related tasks**

- QKD key-relay
- Ciphering
- Prototyping of Quantum Internet protocols

# Thank You

Asier Atutxa, EHU/RedIRIS (asier.atutxa@ehu.eus)

David Franco, EHU/RedIRIS (david.franco@ehu.eus)

Participants in GÉANT GN5-2 WP6 Task 1 - RARE

www.geant.org

Co-funded by
the European Union