61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl

Piotr Rydlichowski

Linking QKD Testbeds in Europe using emulated long-distance links

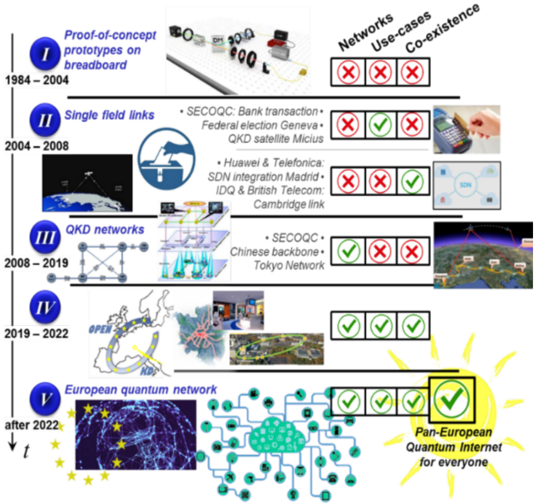
Scope of the work and the publication

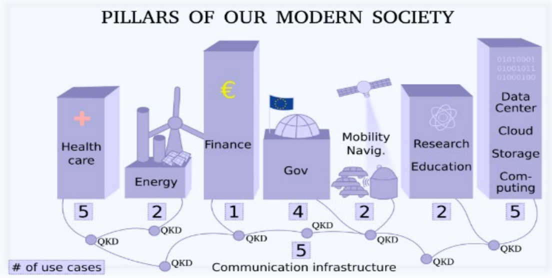
Main goals

- Continue the work undertaken in the OPENQKD project
- Further utilize and extend the OPENQKD testbeds and infrastructure
- Continue the work toward European scale QKD network infrastructure and interconnectivity
- Long-distance QKD links are emulated, the methods used can serve as a blueprint for the secure interconnection of distant QKD networks in the future
- The testbed interconnections are designed to increase the security by utilizing multipath techniques and multiple hybridizations of QKD and post-quantum cryptography (PQC) algorithms
- https://www.mdpi.com/1099-4300/26/2/123

OPENQKD PROJECT

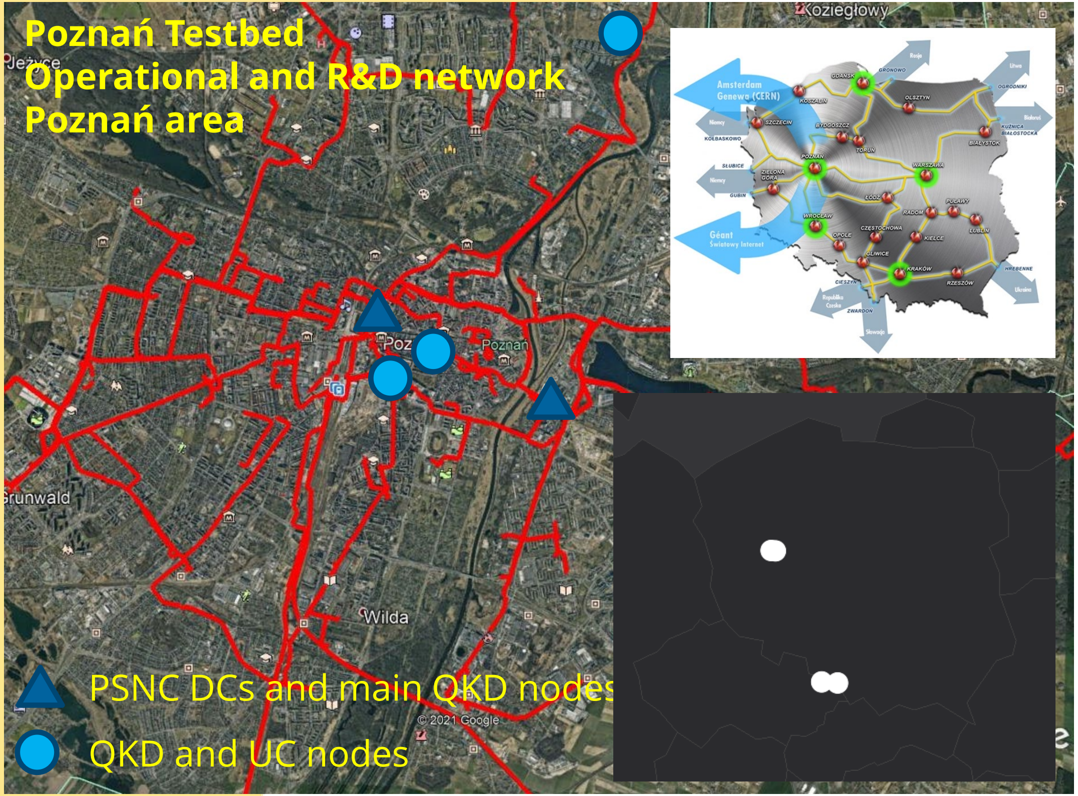
- Construction of QKD testbeds in Europe and implementation of 40 different scenarios for services using QKD technology
- Project start - October 2019, end in 2023
- Multiple main testbeds – Madrid, Berlin , Poznań. Implementation and integration of QKD technology in the existing infrastructure and services of research and operational networks.
- PSNC developed data management and analysis software





Testbed Poznań

- **Infrastructure in place as PSNC** is owner and operator of the infrastructure and network
- **Two QKD links installed and running** tests before the final deployment and use cases implementation
- **Various use cases are beeing prepared:** UC-06, UC-07, UC-08, UC-09, UC-10, UC-11 based on existing services and network. UC with VSB involves **QKD cross-border connection. Reference Time and frequency use case involves long distance connection.**
- **PSNC NOC** is working on implementing the monitoring and logging services for QKD infrastructure and services
- **SDN solutions currently analyzed**
- **Real world operational network** with shared infrastructure for quantum and classical communication and services. Connection point with other operators and several types and manufacturers of transmission equipment and encryptors
- **Direct connection with GEANT** node in Poland, network and services.
- **QKD equipment installed at PSNC DC nodes** and under preparation for use cases
- **QKD equipment installed on Ostrava – Cieszyn crossborder line for HPC use cases with VSB**
- **Joint activities with National project NLPQT – National Laboratory for Photonic and Quantum Technologies**



Poznań Testbed
Operational and R&D network
Poznań area

▲ PSNC DCs and main QKD nodes

● QKD and UC nodes

Assumptions for the QKD testbeds and its interconnections

- The goal of the paper is to demonstrate a feasible connection of present-day European metropolitan-area QKD networks, as developed in OpenQKD and planned in EuroQCI, before long-distance QKD is available and chains of trusted nodes, quantum repeater links, or QKD satellites are installed in Europe.

- In this work, the long-distance QKD connections are only emulated QKD links

- Hybrid PQC and QKD approach

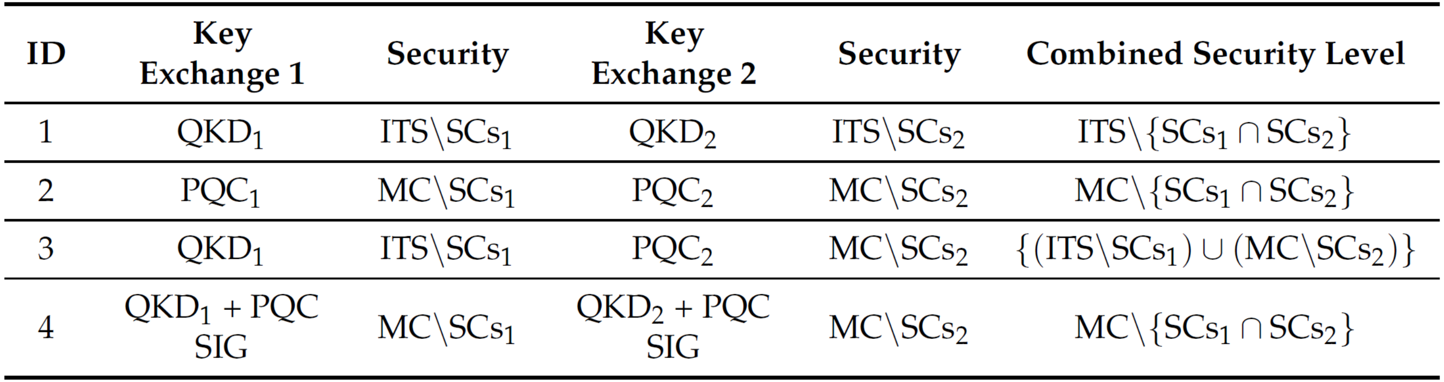
- Two PQC approaches: key agreement ones based on quantum-safe public key encryption-decryption of a secret key, key encapsulation mechanisms (KEM), in what follows PQC KEM, and digital signature ones (SIG), in what follows PQC SIG

- Key forwarding protocols within QKD testbeds

- Side channels analysis: difference between ideal and implemented protocols

- Only the parallel combination of QKD and PQC can increase security, while the sequential combination of protocols can only lead to a security reduction

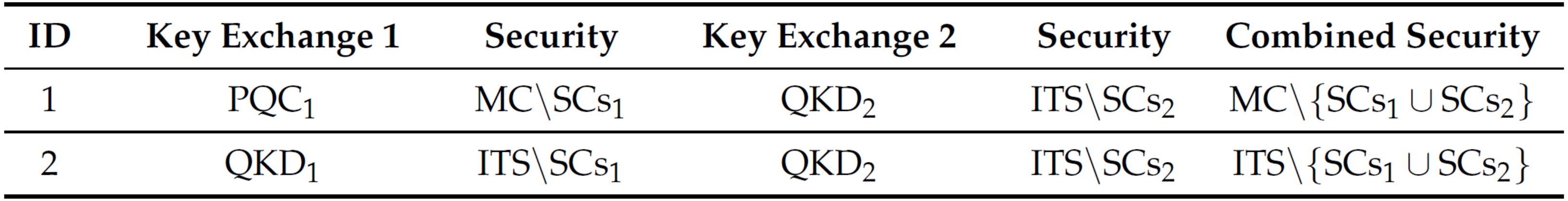
QKD and PQC – hybrid approach



ID	Key Exchange 1	Security	Key Exchange 2	Security	Combined Security Level
1	QKD_1	$\mathrm{ITS}\setminus\mathrm{SCs}_1$	QKD_2	$\mathrm{ITS}\setminus\mathrm{SCs}_2$	$\mathrm{ITS}\setminus\{\mathrm{SCs}_1 \cap \mathrm{SCs}_2\}$
2	PQC_1	$\mathrm{MC}\setminus\mathrm{SCs}_1$	PQC_2	$\mathrm{MC}\setminus\mathrm{SCs}_2$	$\mathrm{MC}\setminus\{\mathrm{SCs}_1 \cap \mathrm{SCs}_2\}$
3	QKD_1	$\mathrm{ITS}\setminus\mathrm{SCs}_1$	PQC_2	$\mathrm{MC}\setminus\mathrm{SCs}_2$	$\{(\mathrm{ITS}\setminus\mathrm{SCs}_1) \cup (\mathrm{MC}\setminus\mathrm{SCs}_2)\}$
4	QKD_1 + PQC SIG	$\mathrm{MC}\setminus\mathrm{SCs}_1$	QKD_2 + PQC SIG	$\mathrm{MC}\setminus\mathrm{SCs}_2$	$\mathrm{MC}\setminus\{\mathrm{SCs}_1 \cap \mathrm{SCs}_2\}$

- Security level of various combinations of different key-exchange technologies in parallel in a symbolic set-theoretic representation. This could be, e.g., discrete variable (DV) and continuous variable (CV) QKD protocols in pure QKD networks, PQC KEM and PQC SIG algorithms in pure PQC networks, and combinations of pairs of technologies for different tasks in mixed networks. QKD implementations are ITS minus (\) side channels (SCs), while the security level of PQC is based on mathematical-complexity (MC) minus SCs. The combined security level of parallel key generation is the union (∪) of the individual security levels. For key exchanges of the same security level this simplifies to this level but minus the intersection (∩) of the SCs. QKD with PSK are assumed. This classification is independent of whether the different technologies are applied over the same or different network paths.

QKD and PQC – hybrid appraoch



ID	Key Exchange 1	Security	Key Exchange 2	Security	Combined Security
1	PQC_1	$\mathrm{MC} \setminus \mathrm{SCs}_1$	QKD_2	$\mathrm{ITS} \setminus \mathrm{SCs}_2$	$\mathrm{MC} \setminus \{\mathrm{SCs}_1 \cup \mathrm{SCs}_2\}$
2	QKD_1	$\mathrm{ITS} \setminus \mathrm{SCs}_1$	QKD_2	$\mathrm{ITS} \setminus \mathrm{SCs}_2$	$\mathrm{ITS} \setminus \{\mathrm{SCs}_1 \cup \mathrm{SCs}_2\}$

- Security level of various combinations of different key-exchange technologies in series in a symbolic set-theoretic representation. The combined security level of serial key generation is the intersection of the individual security levels. For the examples in this table, this is equal to the respectively lower security level minus the union of the SCs.

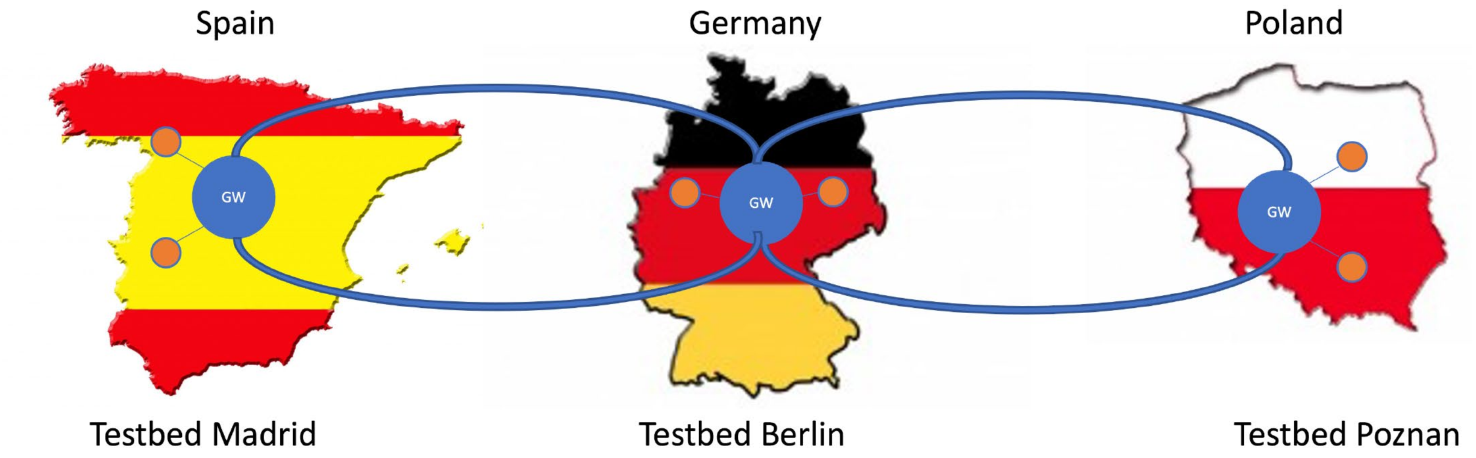
QKD and PQC – hybrid appraoch

- At the moment, the cryptographically most secure combination is a direct, anytoany PQC key exchange combined with an any-to-any QKD key exchange relying on key forwarding.

- A two-path approach, i.e., one that utilizes two different paths, will reduce risks even if a single implementation of a single technology is used.

- Risks will be further reduced if different implementations and, moreover, different technologies, deployed over different paths, are used.

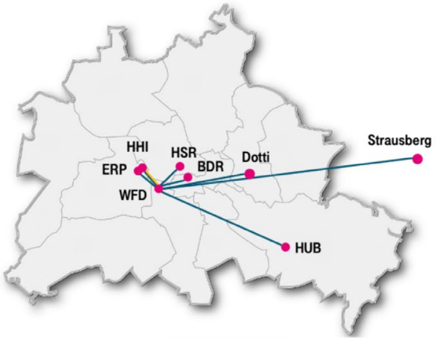
QKD testbeds interconnection scheme

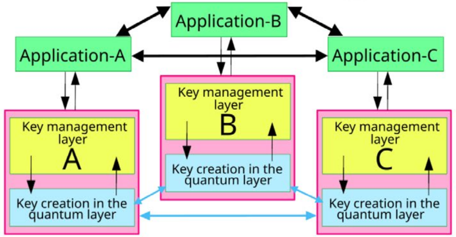


- Connection of the quantum testbeds in Madrid, Berlin, and Poznan with emulated long-distance QKD links.
- The key exchange is indicated by the curved blue lines, which connect dedicated QKD gateway nodes (blue circles) in each testbed.
- The other QKD nodes in the respective testbeds are indicated by orange circles.

Participating QKD Testbeds

Berlin

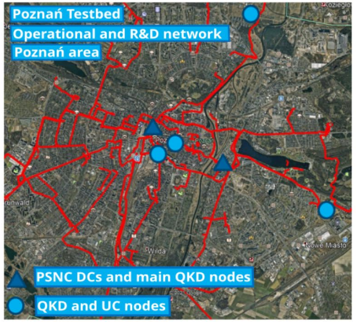


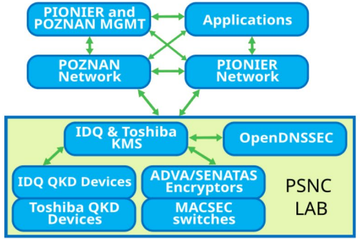


Layers	Equipment
Quantum layer	DV-QKD systems by ID Quantique, DV-QKD systems by Toshiba, PQC key-exchange system developed by Open Quantum Safe [18]
Key-management layer	key-management system (KMS) internally developed by DT, hardware security module (HSM) by Gemalto
Application layer	L1 hardware encryptors by Adva, L3 hardware encryptors by Thales

Participating QKD Testbeds

Poznań





PIONIER and POZNAN MGMT

Applications

POZNAN Network

PIONIER Network

IDQ & Toshiba KMS

OpenDNSSEC

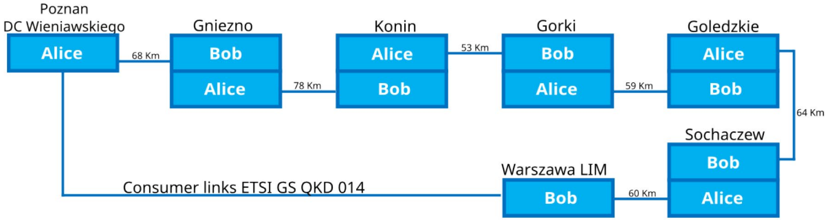
IDQ QKD Devices

ADVA/SENATAS Encryptors

Toshiba QKD Devices

MACSEC switches

PSNC LAB



Poznan DC Wieniawskiego: Alice

68 Km

Gniezno: Bob, Alice

78 Km

Konin: Alice, Bob

53 Km

Gorki: Bob, Alice

59 Km

Goledzkie: Alice, Bob

64 Km

Sochaczew: Bob, Alice

60 Km

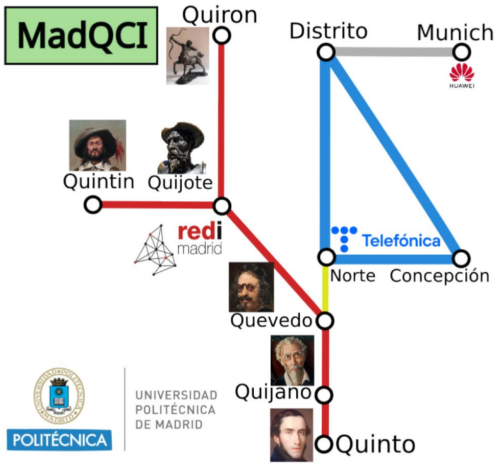
Warszawa LIM: Bob

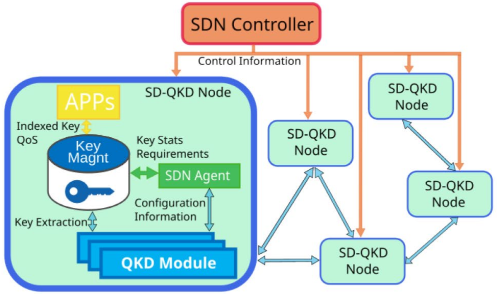
Consumer links ETSI GS QKD 014

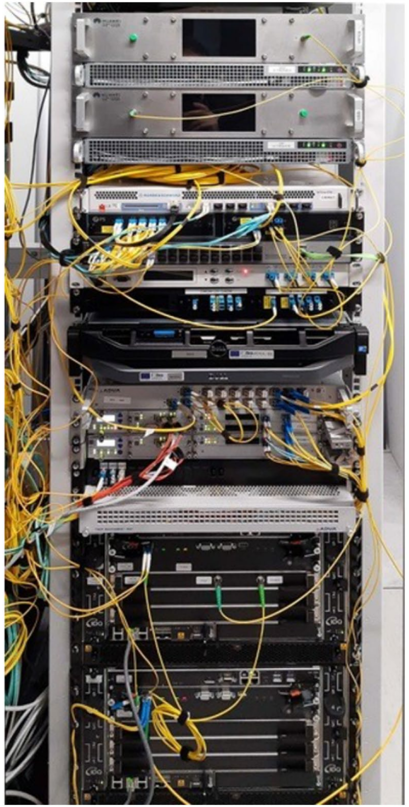
Layers	Equipment
Quantum layer	DV-QKD systems by ID Quantique, DV-QKD systems by Toshiba, PQC key-exchange system from Open Quantum Safe [18]
Key-management layer	Key-management system by ID Quantique, key-management system by Toshiba, security module implemented with open software solutions, OpenDNSSEC
Application layer	L1 hardware encryptors by Adva, L3 hardware encryptors by SENETAS

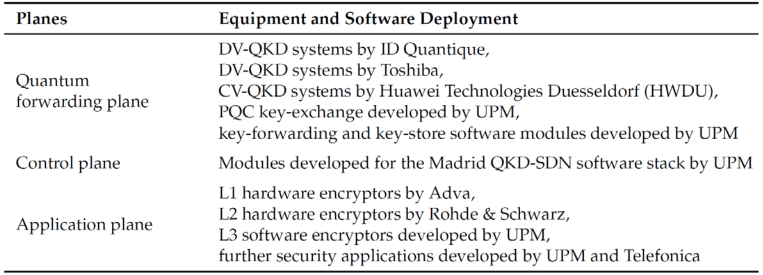
Participating QKD Testbeds

Madrid









Planes	Equipment and Software Deployment
Quantum forwarding plane	DV-QKD systems by ID Quantique, DV-QKD systems by Toshiba, CV-QKD systems by Huawei Technologies Duesseldorf (HWDU), PQC key-exchange developed by UPM, key-forwarding and key-store software modules developed by UPM
Control plane	Modules developed for the Madrid QKD-SDN software stack by UPM
Application plane	L1 hardware encryptors by Adva, L2 hardware encryptors by Rohde & Schwarz, L3 software encryptors developed by UPM, further security applications developed by UPM and Telefonica

Long distance emulated QKD Links

- The long-distance links as of today in Europe can only be realized using a QKD emulation technology (we use PQC methods), since, as already mentioned, neither long-distance QKD, nor trusted repeating chains and/or (the constellation of) QKD trusted satellites are yet deployed on the continent.
- All long-distance links have been realized using PQC KEM protocols and SIG authentication. A two-factor approach was implemented, in which different implementations of PQC KEMs have been used and different physical paths have been employed.
- Different networks, including the terrestrial Internet and commercial satellite systems were used for the demonstrations.
- QKD key forwarding was extended to border node

Long distance emulated QKD Links

- We proposed four border-node methods—**link-based border node, long-haul link-based border node, long-haul application-based border node, and long-haul application-based border nodes with multi-path diversity**—that we have deployed on selected points of presence (PoPs) of the various metro networks. (Note that two metro networks, the Telefonica and REDIMadrid ones, can be seen as a part of the Madrid network, which logically includes also the Munich single link. These three Madrid network segments can be seen as three independent networks).

- The four methods have a purely experimental purpose, but they may be viewed as a demonstrator or rather an emulator for a trans-European long-haul QKD network.

Link-Based Border Node – Method 1

- This method, specifically as presented here, is appropriate for connecting QKD networks with similar or even identical architectural designs.
- It was used in MadQCI to connect the networks of two different telecommunication providers, the REDIMadrid QKD network and the Telefónica QKD network
- From an operational perspective the link-based border node method appears to be analogous to the operation of a regular metro network QKD link. However, taking into account that the link connects two different QKD networks, we extended the functionality of the quantum forwarding plane (the set of functionalities and devices required to forward the QKD keys through the network) to be able to transport the final keys from one administrative domain to another.
- The border nodes are the only ones allowed to communicate with external networks, and typically this operation requires a strict service level agreement and a corresponding negotiation protocol
- Once the key has been transported from the source node in one network to the destination node in the other, an E2E secure communication can take place

Long Haul Link-Based Border Node – Method 2

- This method is logically similar to the previous one, and it is adapted to the case in which no distant QKD keys are available.
- It has been used to connect two QKD networks: one is a MadQCI segment, the Telefónica Network, and the other is the network segment represented by the remote QKD link at the HWDU facilities in Munich.
- The long distance between both network segments cannot presently be bridged by true QKD links. As an alternative, and since both segments are based on the same SDN paradigm and design, a long-distance QKD link is emulated using PQC between the corresponding border nodes at Telefonica Research in Distrito and the Munich Research Center of HWDU,
- The emulated long-distance QKD link runs two distinct PQC KEM protocols, the outputs of which are hybridized, as in Method 1, to create a border node to border node key (i.e., through the emulated distant QKD link)
- The rest of the process is strictly analogous to that described in Method 1
- There is only one SDN controller managing all the QKD trusted nodes in the Telefónica segment and the Munich link as if this were the same physical network
- Link was implemented using the ETSI GS QKD 004 key delivery interface because of the quality of service options offered by this API. It allows us to emulate this link choosing a constant key rate. We selected 256bps and a key length of 32 bytes.

Long Haul Application-Based Border Node – Method 3

- This approach is oriented to the interconnection of networks that are different in terms of their design, for example, networks based on the traditional QKD network layered architecture (Berlin, Poznan), with a network based on a different architectural paradigm, such as, e.g., a QKD-software-defined network (Madrid).

- The idea is to have an application service running on the authorized nodes of each network.

- This application service is administrated in each domain by the respective network operator.

- Due to the long distance between the testbeds, both sides of the application establish an emulated QKD link (a PQC link instead of a QKD one), albeit in a two-factor manner, which is based on the hybridization of two implementations but over the same path

Long Haul Application-Based Border Node – Method 3

The following steps are required

1. Retrieve random numbers (RNDs) and matching identifiers RNDIDs from a (quantum) random number generator ((Q)RNG).
2. Encrypt the random numbers using different PQC KEM algorithms, independently and hybridize the outputs to a single key string.
3. Add meta information, for example the RNDID, a key validity period or the name of the sending node is added to the encrypted random number. The entire package is finally signed using a different PQC SIG algorithm for each KEM choice.
4. After data serialization, the data package is sent from one border node to the other border node.
5. Finally, the sending side pushes the encryption key, the identifier and the corresponding meta data into a KMS that may be a HSM or an encrypted file share.

Long Haul Application-Based Border Node – Method 3

At the receiving node, the key exchange protocol consists of the following steps

1. After the reception of a message the sender is identified by its IP address.
2. The message is deserialized and the signature of the sender is validated using the PQCSIG algorithms. The appropriate public SIG key(s) of the sender is (are) determined from the IP address recorded at step 1.
3. If validated, the receiver de-hybridizes and subsequently decrypts the encrypted random number, the identifier and corresponding metadata.
4. Finally, the receiving side pushes the transported key, the identifier and the corre sponding meta data into an KMS

Long Haul Application-Based Border Node – Method 3

- The border node service is running constantly, and it stabilizes a constant PQC link where randomized keys could be obtained by several methods (one of them being the use of a QRNG).

- A quantum-safe long-haul application-based border node was implemented as a regular QKD key consumer application on top of the KMS layer using ETSI GS QKD 004 (ETSI GS QKD 014 could also be appropriate). This approach was designed for the key exchange between different (architectural and functional) networks

- In future, when direct QKD links between the border nodes of different QKD networks will be available, (one of) the consumer-application(s) supporting this method, will simply utilize the direct QKD link key as the key source and encrypt the payload-key by a symmetric ITS method, i.e., a one-time pad.

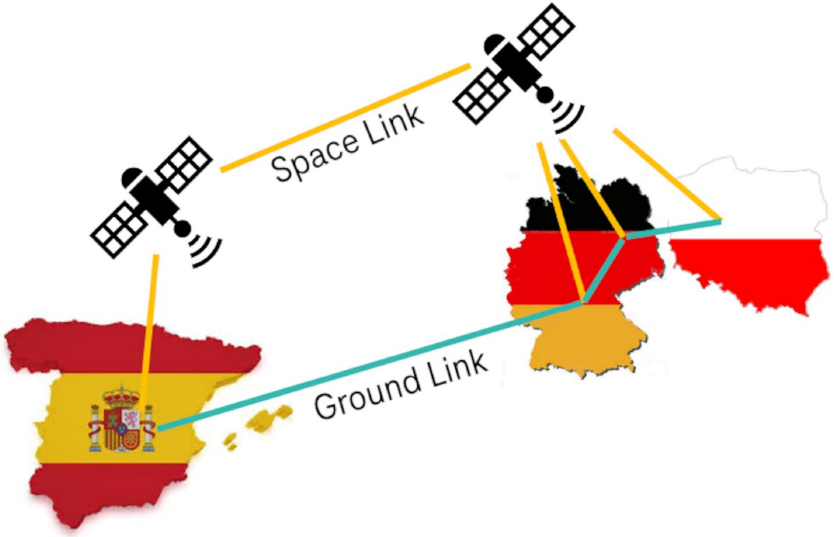
Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4

- This approach adds multi-path security to the previous one using two disjoint network links. We used the public Internet or the “ground link” and a satellite-based link via the commercial Iridium network, or the “space link”.

- The long-distance forces us to use emulations of QKD. A two-path algorithm, based on different PQC KEM and SIG protocols is used. It differs from the one outlined in the Method 3 in the sense that non-coinciding random number strings are sent in this twofactor version along different routes and subsequently these are combined, rather than encrypting a single random string with different methods and then hybridizing the result.

- Similarly, if (one of) the SIG or KEM implementations is broken, this might result in a denial-of-service attack as the final keys between the distant nodes might not coincide or the messages may be considered unauthorized.

Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4



- The disjoint network is realized by a “space link” via the Iridium network and a “ground link” via the public Internet. The network connects the gateway nodes of the Madrid, Berlin, and Poznan QKD testbeds. The Munich Research Center of Huawei in Germany serves as a pseudo-internal node of the Madrid network.

Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4

The PQC-based two-path key exchange protocol involves the following steps for the sending node:

1. Retrieve two random numbers (denoted by RND1 and RND2) and a matching identifier per RND (denoted by a single RNDID) using a (Q)RNG. The index 1 is liaised to the space link, whereas the index 2 denotes the “ground link”.
2. Encrypt the random numbers using different PQC KEM (key encapsulation mechanism) algorithms. Depending on the chosen path, a different public KEM key is applied. Any appropriate KEM algorithm may be used. We used Kyber on the space link and NTRU on the ground link, because these algorithms showed good performance with current implementations.
3. Meta-information, for example the RNDID, a key validity period, or the name of the sending node is added to the encrypted random number. The entire package is finally signed using a different PQC SIG algorithm for each network path. Any appropriate SIG algorithm may be used. We used Falcon on the space link and Dilithium on the ground link.
4. After data serialization, one key package is sent via the space link, the other key package via the ground link.
5. On successful data transmission, the sending side combines the two random numbers RND1 and RND2 to compute an encryption key (KEY) using a key derivation function (KDF), so that KEY = KDF(RND1, RND2, PSK), where PSK is some (possibly empty) pre-shared key string. Any KDF standardized by NIST or ETSI may be chosen. (In case real QKD links and not only emulated QKD links are used, this choice of KDF must be restricted to functions that ensure the epsilon-composability of the output; e.g., a simple XOR-ing function can be considered.) The KEYID is set identical to the RNDID and will be required for the key negotiation protocols. Finally, the sending side pushes the encryption key, the identifier, and the corresponding metadata into a KMS.

Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4

At the receiving node, the key exchange protocol consists of the following steps:

1. After the reception of a message on either network pathi, i = 1, 2, the sender is identified by its IP address.
2. The message is deserialized and the signature of the sender is validated using the PQC SIG algorithm. The appropriate public SIG key(s) of the sender is (are) determined from the IP address recorded at step 1.
3. If validated, the receiver decrypts the encrypted random number RNDi, the identifier RNDIDi, and the corresponding metadata using the PQC algorithm KEMi.
4. The decrypted random numbers, their identifiers, and the metadata are then sent to a queue for further processing.

Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4

- The PQC algorithms are compiled into openssl.
- A PQC-enabled version of the nginx web server with multiple workers is used and the Python code uses multithreading to increase the performance
- The security system preserves the secrecy of the final key, as long as a single path of the disjoint network paths remains secure.
- The security of the solution can even be increased by adding more disjoint paths and securing the key exchange using different PQC algorithms. As well as the combination of satellite and terrestrial networks, there are other commercial networks which are disjoint, for example, the networks of competing mobile network service providers or European research fiber networks or commercial fiber networks. Once existing, even a satellite QKD or long-haul quantum optical key exchange link may be added to make the solution information theoretically secure (albeit by a more careful selection of the KDF, as mentioned) with a significant side channel reduction

Long Haul Application-Based Border Nodes with Mulit-Path Diversity – Method 4

- The long-haul application-based border nodes were implemented in the Berlin, Poznan, and Madrid testbeds on specific QKD trusted nodes, using physical servers.

- The Iridium “space network” and the “Internet” are used to exchange the encryption keys over disjoint network paths. Using a virtual machine with two CPUs and 16 GB RAM, the presented software solution manages to transfer 4 kBits (which corresponds to 16 AES-256 keys per second). The virtual machine was equipped with a PQC-enhanced web server and client applications running the key exchange. To do so, and to compensate for the long latency of about 600 ms per request, the best performance was achieved when sending blocks of 50 to 75 keys per https session. The bottleneck of the implementation turned out to be the recombination function to grab the two random numbers and apply the KDF.

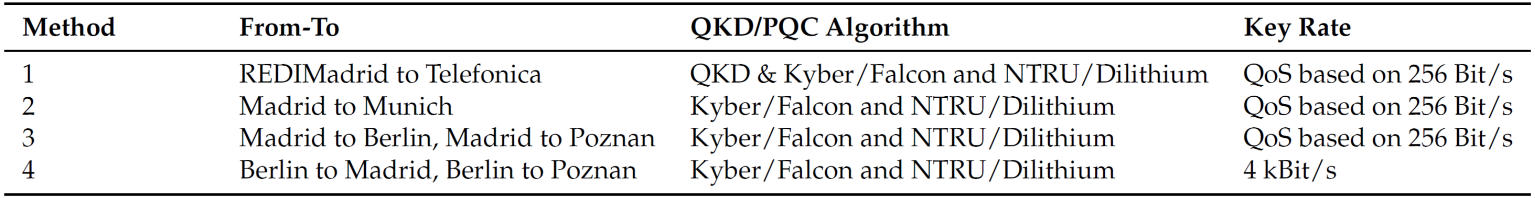
- The usage of an LEO (low Earth orbit) satellite constellation, like Star Link, may also increase the performance of the implementation

Experimental results

- Each border node (as, in fact, any trusted node) was equipped with a computer system and software to run the PQC-enabled key exchange protocols

- The networks were linked by a logical, classical VPN network

- By adding more CPU threads to the key exchange application, the performance can easily be scaled



Method	From-To	QKD/PQC Algorithm	Key Rate
1	REDIMadrid to Telefonica	QKD & Kyber/Falcon and NTRU/Dilithium	QoS based on 256 Bit/s
2	Madrid to Munich	Kyber/Falcon and NTRU/Dilithium	QoS based on 256 Bit/s
3	Madrid to Berlin, Madrid to Poznan	Kyber/Falcon and NTRU/Dilithium	QoS based on 256 Bit/s
4	Berlin to Madrid, Berlin to Poznan	Kyber/Falcon and NTRU/Dilithium	4 kBit/s

Key Forwarding through Border Nodes

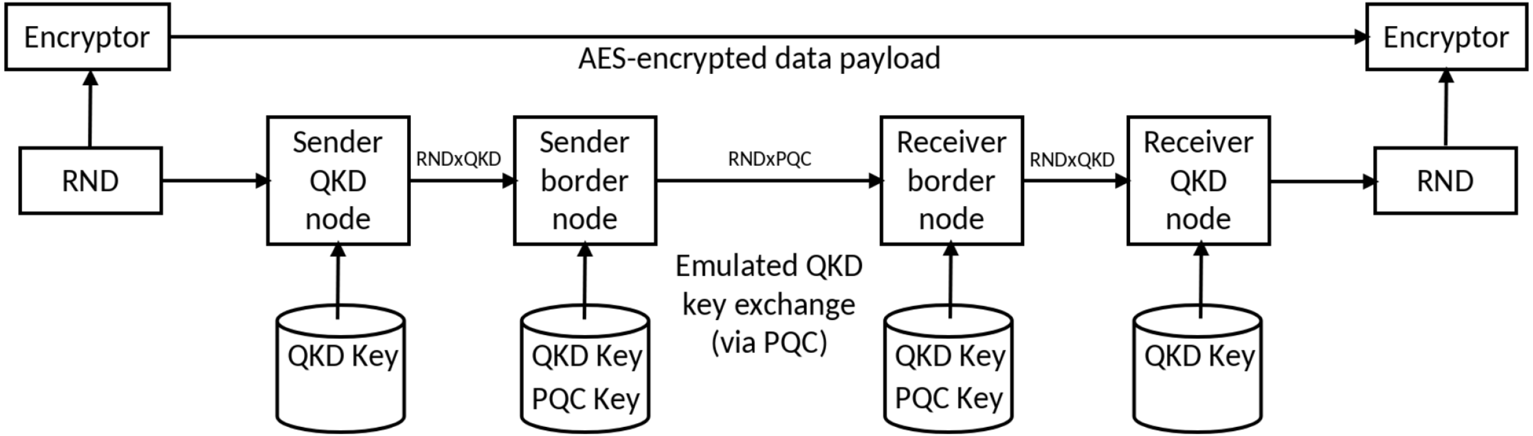
- We present various solutions to realize a border node key exchange between individual European QKD deployments, making use of QKD and PQC as the applied emulations of QKD.

- This yields an overarching architecture, where the border nodes are deployed to interconnect the QKD deployments.

- Random numbers are forwarded from a source QKD node to the border node (communication secured by QKD keys), from there to another border node of a target QKD infrastructure (secured for now by an emulated QKD, or a QKD satellite in the future), and further on to a target QKD node. As a result, the source and the target QKD nodes share the same random number, which they may utilize as, e.g., a secure key to, for example, encrypt the classical data payload.

- The distant link (border node integration) was realized using PQC links due to the lack of appropriate quantum technology.

Key Forwarding through Border Nodes

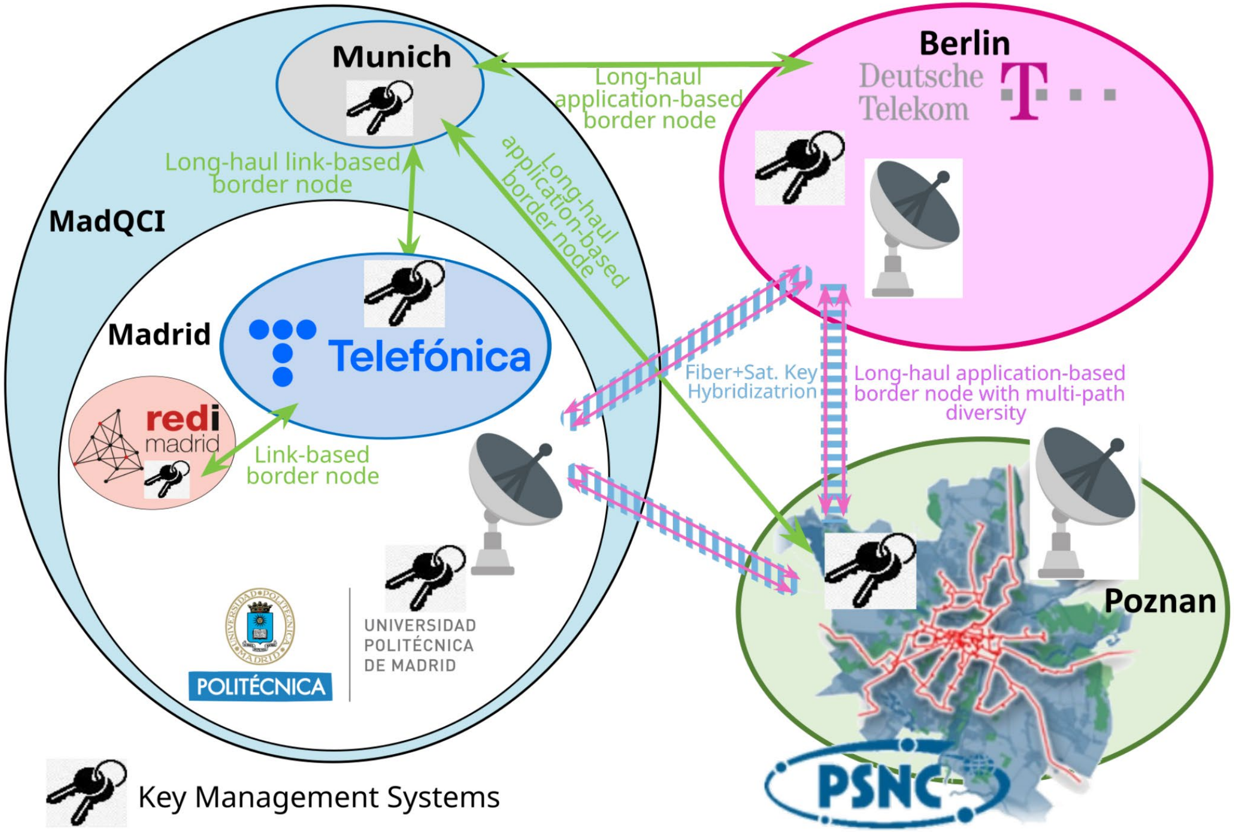


- Integration of an emulated QKD key-exchange system into a QKD architecture.
- The keys of the emulated QKD key exchange are stored in the local key store of the border nodes.
- A sending QKD node forwards a random number through the trusted-node chain of the senders border node and the recipients border node to the receiving QKD node.
- The random number is either directly used as a final secure key or two random numbers, transferred across disjoint network links, are combined using a KDF for the final secure key.

Key Forwarding through Border Nodes

- The resulting network is fully meshed.
- Each gateway node operates a PQC key exchange server that listens for incoming connections.
- Additionally, each gateway node could initiate a key exchange through the key exchange client, yielding a bi-lateral key exchange.
- The testbeds integrate the PQC key exchange by pushing the keys, their identifiers, and their metadata directly into the KMS at every location, where they can be consumed by encryptors or applications via the ETSI GS QKD 004 or 014 API and an appropriate key negotiation process.

Key Forwarding through Border Nodes



Munich
Berlin
Deutsche Telekom
Long-haul application-based border node
Long-haul link-based border node
Long-haul application-based border node
MadQCI
Madrid
Telefónica
redi madrid
Link-based border node
Fiber+Sat. Key Hybridizatrion
Long-haul application-based border node with multi-path diversity
Poznan
UNIVERSIDAD POLITÉCNICA DE MADRID
POLITÉCNICA
PSNC

Key Management Systems

Hybrydization of All Generated Keys

- We propose to integrate a hybridization scheme to compute the hybrid final keys at each network node
- In the present work, the hybridization follows the recent Muckle scheme that puts forward a hybrid method for authenticated key exchange (specifically, it is based on a secure hybridization, i.e., combination, of several keys of QKD, PQC, and PKC origin, and additionally, the authentication of the key distribution using PSK, instead of PQC SIG), and relies on extended hybridization involving multiple media/paths
- The key exchange module between PoPs was modified to manage not only the QKD keys, but also the PQC ones.
- The systems also allow the use of several key exchange modules in parallel, even with the same PoPs.
- The KMS systems receive the keys (QKD and PQC or any other key exchange mechanism) in a transparent manner from these key exchange modules, so the KMS can establish different quantum-safe key exchange sessions with other PoPs, using QKD links, PQC links, or a combination of both in a simple way.
- Key exchange modules run in parallel on each node delivering keys to the KMS.

Hybrydization of All Generated Keys

- The KMSes only receive notice of a new link between two PoPs. This design enables the generic integration of additional links, and the keys generated by PQC are internally managed by a KMS exactly as any key material generated by QKD.
- All these interfaces can be seen as quantum-safe key delivery interfaces, whereby (Q)RNG serves as the key source
- The key hybridization process is performed by applying a hybridization KDF.
- The key hybridization process is performed as an internal process on the KMS that manages different internal key stores.
- The key hybridization process needs to process the appropriate key bits so that a new, hybrid key is computed, stored, and handed over to the applications and encryptors.
- Alternatively, hybridization may be left to the application, since the application oversees enforcing the required security level itself by picking a key or a combination of keys exchanged under the right security paradigm

PSNC

Poznan Supercomputing and Networking Center

61-139 Poznań
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl