Annex A:

Draft new Recommendation ITU-T Y.QKDN-rsfr

Framework of quantum key distribution network resilience

Summary

For quantum key distribution network (QKDN), this recommendation describes a framework of QKDN resilience. This recommendation describes the overview of QKDN resilience, models and requirements of QKDN protection and recovery. It also includes different use cases of QKDN resilience in the appendix.

Keywords
Quantum key distribution (QKD); QKD network (QKDN); QKDN resilience; framework; requirement.

Table of Contents

Draft new Recommendation ITU-T Y.QKDN-rsfr

Framework of quantum key distribution network resilience

1. Scope

This Recommendation describes a framework of QKDN resilience. It gives an overview on QKDN resilience with its related models, including protection and recovery. And it specifies requirements of QKDN multiple layers to support QKDN resilience.

In particular, the recommendation includes:

- Overview of QKDN resilience;
- Models of QKDN resilience;
- Requirements of protection for QKDN resilience;
- Requirements of recovery for QKDN resilience.

Appendix I illustrates use cases of QKDN resilience.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), *Security framework for quantum key distribution networks*.

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Framework for Networks to support Quantum Key Distribution*.

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the Quantum Key Distribution network.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Key management for quantum key distribution network*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Control and Management for Quantum Key Distribution Network.*

3. Terms and definitions

3.1. Terms defined elsewhere

This recommendation uses the following terms defined elsewhere:

3.1.1 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.2 quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

3.1.3 **key manager (KM)** [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.4 **quantum key distribution link (QKD link)** [ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.5 **user network** [ITU-T Y.3800]**:** A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

3.1.6 **key relay** [ITU-T Y.3800]: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

3.2. **Terms defined in this Recommendation**

None.

4 Abbreviations and acronyms

This chapters describes all the abbreviations and acronyms used in the recommendation.

QKD	Quantum Key Distribution
QKDN	QKD Network
KM	Key Manager
KMA	Key Management Agent
KSA	Key Supply Agent

5 Conventions

In this Recommendation:

The keywords “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is recommended to” indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords “can optionally” indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor’s implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of QKDN resilience

The capability against failures is of positive significance for the construction of QKDN. QKDN protection and recovery aim to maintain the continuous key supply in the event of QKD failures. This recommendation specifies a framework of QKDN resilience, mainly from the aspects of protection and recovery of key supply, which is supported by functions in multiple layers based on the functional requirements of QKDN in [ITU-T Y.3801] and functional architecture of QKDN in [ITU-T Y.3802]. The consideration on QKDN resilience is also based on the functions in multiple layers specified in [ITU-T Y.3803] and [ITU-T Y.3804].

NOTE 1 – Beyond protection/recovery specified in this Recommendation, there are other options to support QKDN resilience.

Providing the continuous key supply for user network is important in QKDNs. Different kinds of failures could be occurred in a QKDN, that affect or even interrupt the key supply. This recommendation focuses on how to protect the QKDN from key supply interruption or how to recover the key supply. In QKDN, the failures in different layers could be correlated and the immediate effects are reflected in key-supply anomalies. For example, if the communication on quantum channels is interrupted for reasons such as optical fibre cuts, key supply will be broken off caused by key-generation suspending. And the key generation through the impaired channels will also be interrupted. When such failures accumulate, obvious impairment such as QoS degradation will occur for the user network services, while for QKDN, it can be a systematic interruption. Thus, this recommendation describes a framework of QKDN resilience to support the continuous key supply under failures.

This Recommendation considers the following models of QKDN resilience.

1) QKDN resilience supported by protection;

2) QKDN resilience supported by recovery;

In the following clauses, the recommendation specifies models of QKDN resilience, which could be supported with quantum layer, key management layer, QKDN control layer, and QKDN management layer.

7 Models of QKDN resilience

In this recommendation, protection and recovery are specified to support QKDN resilience.

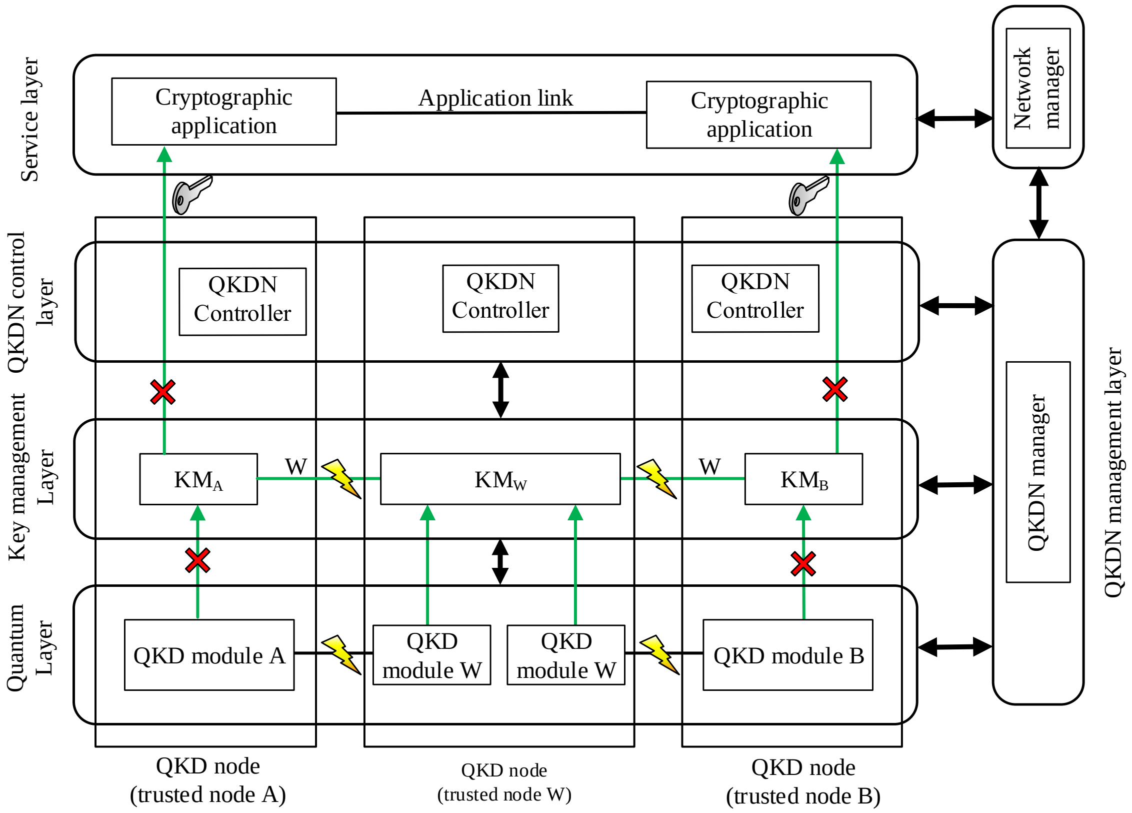

Figure 1 – Key-supply failures in QKDN

As shown in Fig. 1, the key supply to the cryptographic applications can be interrupted by potential failures occurring in either the KM layer or the quantum layer.

7.1 Protection of key supply in QKDN

[Editor's note: Some descriptions or notes could be added to clarify the implementation of QKD module A-2, that whether the protection at the quantum layer is achieved by optical switching or different modules within the same QKD node, or whether both are involved.]

QKDN protection provides additional QKD services for stable key supply through operations of multiple layers, such as the allocation of backup resources. Functional enhancement in multiple layers could be supported in QKDN. In this recommendation, 1:1 and 1:n protection are specified to support QKDN resilience. The QKD services on alternative paths could support the prevention of potential key supply interruptions. And the following terms represent the status of QKD paths in the scenario of QKDN protection.

- QKD working path (W): a QKD path consisting of QKD links that normally provisioning keys.
- QKD protection path (P): an alternative QKD path that pre-set for protection.
- QKD protected path: a QKD working path that matched with a QKD protection path. When the failure occurs on the QKD protected path, the key supply of it would be replaced with the QKD protection path.

A protection path can be shared with single or multiple working paths as 1:1 or 1:n protection. The QKD services over the protection path can be utilized to enable continuous key supply for single or multiple impaired working path(s). When there is no failure in protected paths, the QKD services through the protection path are available for other cryptographic application until the failure or anomalies occurs.

As shown in Fig. 2, a model of 1:1 protection in QKDN is provided. For the 1:1 protection, a QKD protection path A-P-B is pre-set for QKD working path A-W-B, while the QKD links A-P and P-B through the protection path are available for other application when there are no failures or anomalies in the working path A-W-B. When the QKD service over A-W-B is impaired, it switches to the key supply of protection path A-P-B. In the process, the supply of keys for other applications may be interrupted.

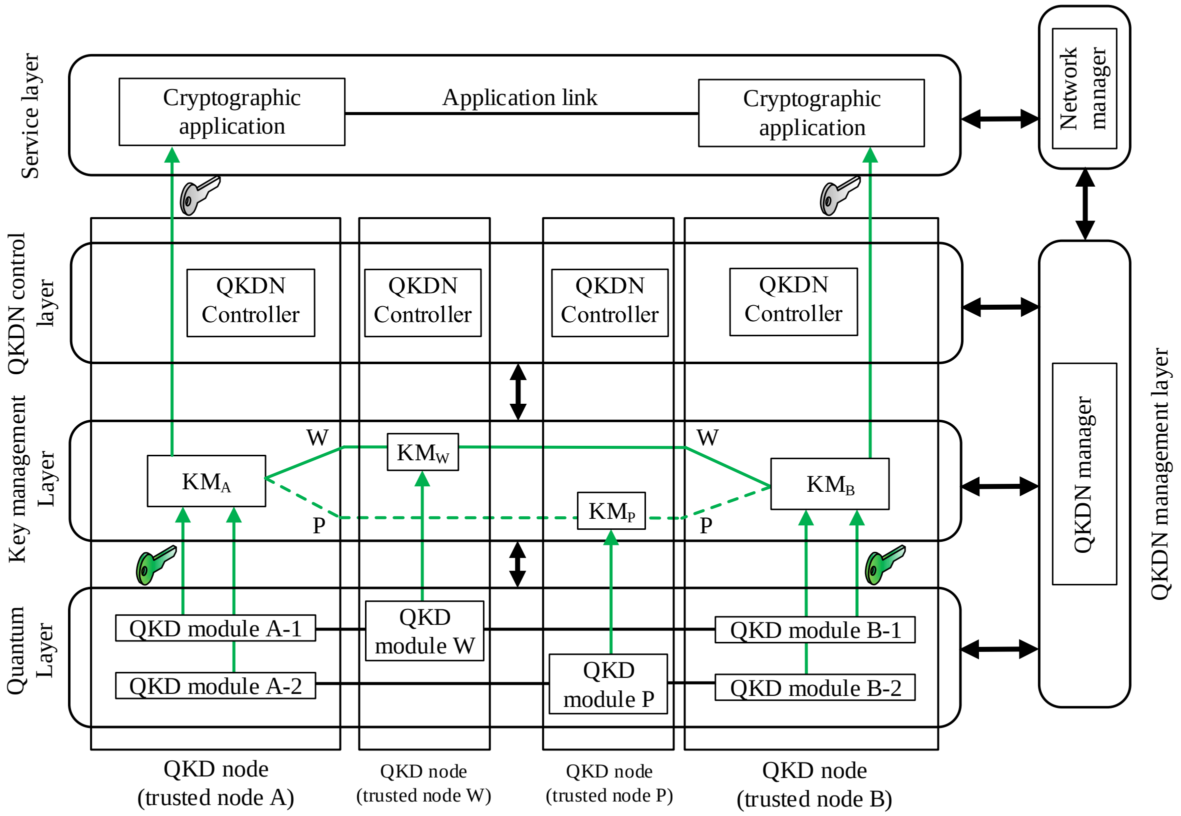

Figure 2 – A model of 1:1 key-supply protection in QKDN

NOTE 1 – The QKD modules (QKD module W and QKD module P) connecting QKD modules A and B are abbreviated for simplification.

As shown in Fig. 3, a model of 1:n protection in QKDN is provided. For the 1:n protection, a QKD protection path A-P-B is pre-set for multiple QKD working paths. When one of the QKD protected paths is impaired with its QKD service, it switches to the key supply of protection path A-P-B, where the keys could be further synchronized. In the process, the supply of keys for other applications over the protection path may be interrupted.

NOTE 2 – To support QKDN resilience with 1:1 protection and 1:n protection, relevant key-supply interruption and switching overheads should be taken into consideration.

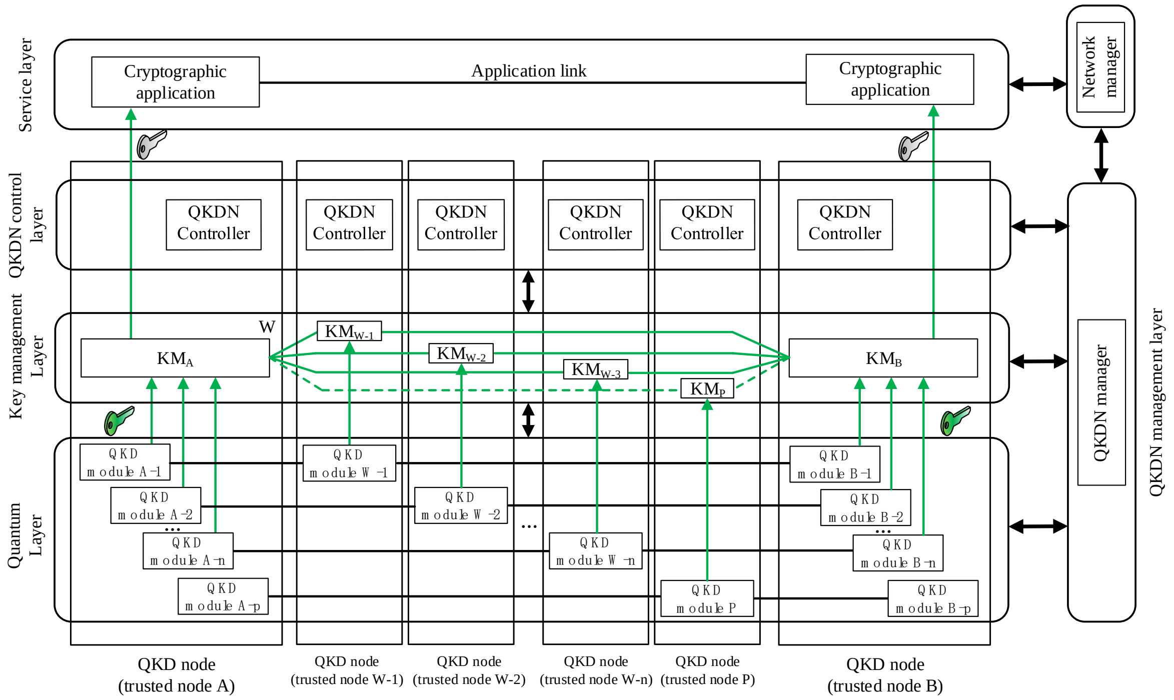

Figure 3 – A model of 1:n key-supply protection in QKDN

7.2 Recovery of key supply in QKDN

QKDN recovery aims to recover the impaired key supply of QKDN through functions of multiple layers. It searches for the available QKD services that gradually recover the key supply without pre-reserving alternative resources. Functional enhancement could be supported by entities in QKDN multiple layers. Specifically, QKDN provides the function of re-routing for key-supply recovery as shown in Fig. 4.

- QKD re-routing path: a QKD path consisting of QKD links that searched for key-supply recovery.

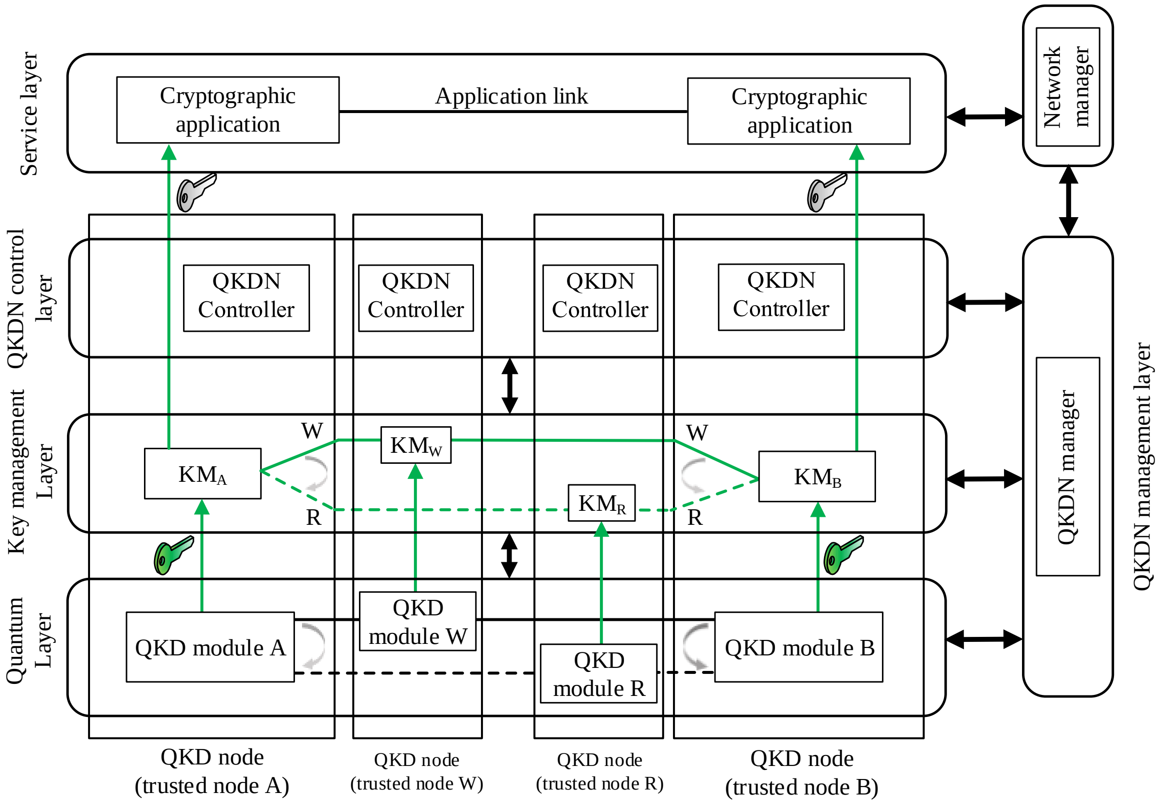

Figure 4 – A model of re-routing for QKDN resilience

When there occurs the key-supply failure in QKDN, recovery tries to maintain the continuous key supply of the impaired QKD service(s) through searching for the QKD re-routing path. It can replace the impaired QKD service(s) with other available QKD paths. As a result, the interrupted key supply to cryptographic application can be recovered. Recovery could be achieved by QKDN control layer and QKDN management layer. Based on the scale of key-supply failure(s), the overheads for recovery can be different. In general, the scenarios of QKDN recovery can be divided into recovery for single failure and recovery for multiple failures.

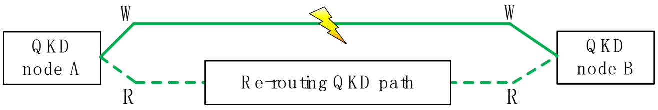

Figure 5 – A scenario of recovery for single failure in QKDN

As shown in Fig. 5, a scenario of recovery for single failure in QKDN is provided. When the specific QKD link A-B is impaired, the QKDN will search for a QKD re-routing path with sufficient resources to replace the impaired key supply.

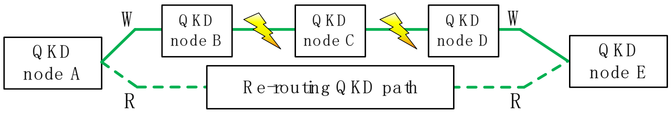

Figure 6 – A scenario of recovery for multiple failures in QKDN

As shown in Fig. 6, a scenario of recovery for multiple failures in QKDN is provided. For the scenario of recovery for multiple failures, QKDN can perform the recovery from a global perspective (e.g., recovery of multiple failures with single re-routing path). When the specific QKD services over QKD links B-C and C-D are impaired, the QKDN will search for a QKD re-routing path between node A and node E with sufficient resources to replace the impaired key supply.

NOTE 1 – To support QKDN resilience with recovery, the overhead including time delay with re-routing should be taken into consideration.

8 Requirements of protection for QKDN resilience

The protection for QKDN resilience can be support with functions in multiple layers, including relevant requirements or options in quantum layer, QKDN control layer and QKDN management layer.

In quantum layer,

- QKDN is recommended to pre-set additional QKD paths as the QKD protection paths for 1:1 or 1:n protection in quantum layer;
- The QKD protection path is recommended to have an equivalent QKD ability with the matched QKD protected path(s).

In QKDN control layer and QKDN management layer,

- QKDN is required to record the matchup between QKD working paths and QKD protection path in QKDN management layer;
- QKDN is required to monitor the status of key supply and respond to the failures in QKDN control layer and QKDN management layer;
- QKDN is recommended to formulate the priority policies for QKD protected paths according to the users' requirements in QKDN management layer.

9 Requirements of recovery for QKDN resilience

Recovery can be support with functions mainly in QKDN control layer and QKDN management layer:

- QKDN is required to monitor the status of key supply and respond to the failures in QKDN control layer and QKDN management layer;
- QKDN can optionally record the operations of recovery to update the status of QKD links and modules in QKDN control layer and QKDN management layer;
- QKDN can optionally perform the recovery methods (i.e., for single failure or multiple failures) according to the policies and failure situation in QKDN control layer and QKDN management layer;
- QKDN can optionally search for multiple QKD paths (i.e., multi-path key provisioning) to enable recovery of impaired key supply;
- QKDN is recommended to search for the QKD re-routing path for recovery within the toleration time of the cryptographic application.

Appendix I

Use cases for QKDN resilience

(This appendix does not form an integral part of this Recommendation.)

The continuous key supply under failures is important in QKDN. With functional requirements and architecture specified in Y.3800 to 3804, the QKDN resilience can be supported by multiple layers. Figures 7-9 show several use cases of protection and recovery as well as corresponding operations with the support of QKDN multiple layers.

The use cases of protection, and recovery are described in this appendix.

I.1 Use case of protection in QKDN

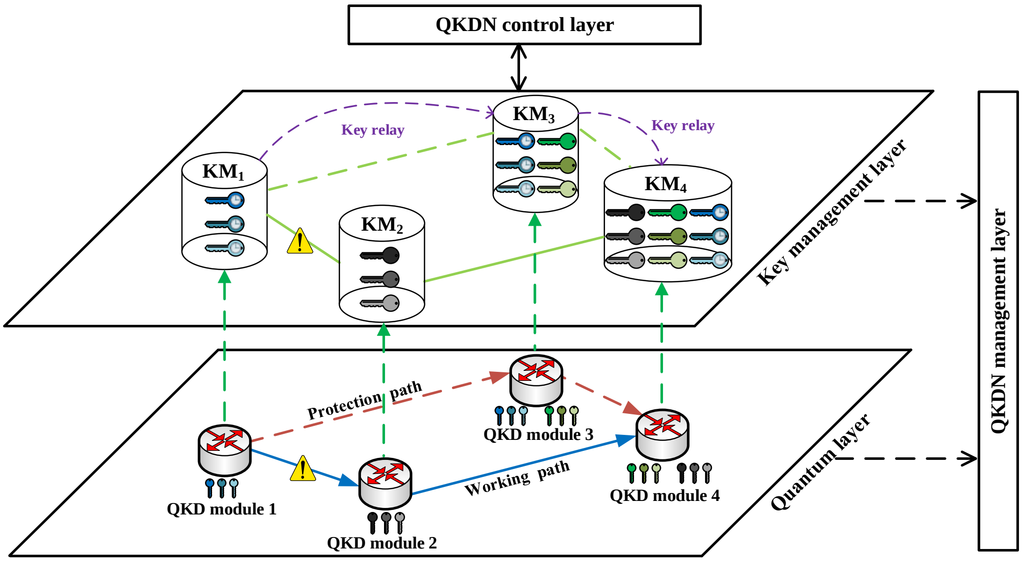

Figure 7 – Case 1 for QKDN resilience with 1:1 or 1:n protection

Case 1) The working path through QKD modules 1, 2 and 4 supplies keys to cryptographic application A. To avoid the interruption of the QKD process caused by the failure of specific QKD path, 1:1 or 1:n protection could be adopted as follows:

For the 1:1 protection, an alternative QKD path (i.e., the path goes through QKD modules 1, 3 and 4) is pre-set as the QKD protection path. QKD links 1-3 and 3-4 through the QKD protection path are available to other cryptographic applications when there are no failures. When the QKD protected path 1-2-4 is impaired, leading to the interruption of key supply, it switches to the path 1-3-4 for synchronized key supply to cryptographic application A.

For the 1:n protection, the alternative QKD path is pre-set as the QKD protection path for multiple QKD working paths. Thus, when one of the QKD protected paths is impaired, it can switch to the protection path for synchronized key supply. The priority of the utilization of keys for different protected paths will be set in the QKDN management layer.

I.2 Use cases of recovery in QKDN

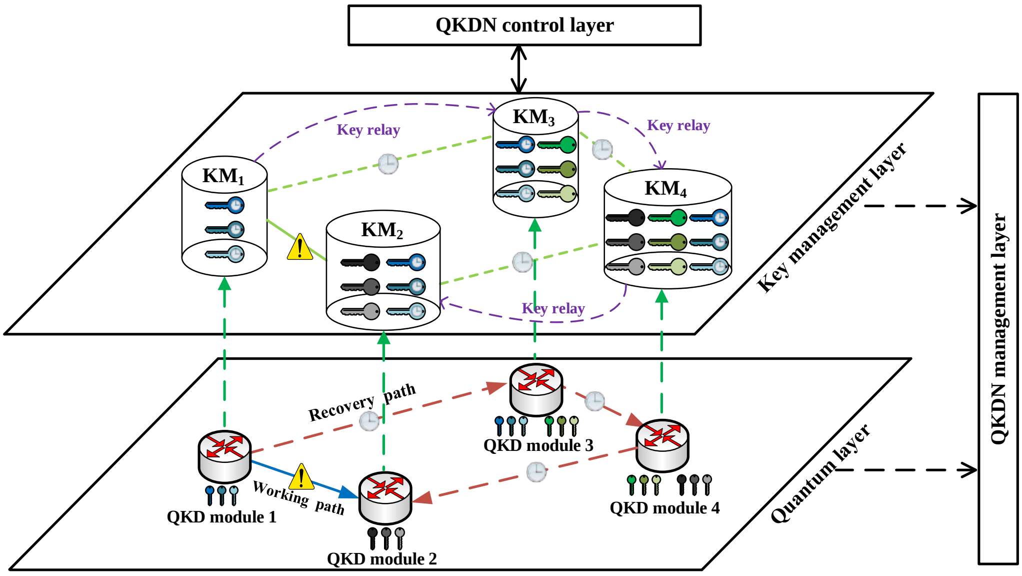

Figure 8 – Case 2.1 for QKDN resilience with recovery for single failure

Case 2.1) The working path through QKD module 1 and QKD module 2 supplies keys to cryptographic application A. If the QKD link from QKD module 1 to QKD module 2 is impaired, the related QKD process could be interrupted. For the recovery of single failure, a QKD rerouting path will be searched for synchronized keys to recover the impaired key supply of application A, i.e., the QKD path which goes through QKD modules 1, 3, 4, 2. The time delay and other overheads caused by recovery should be considered.

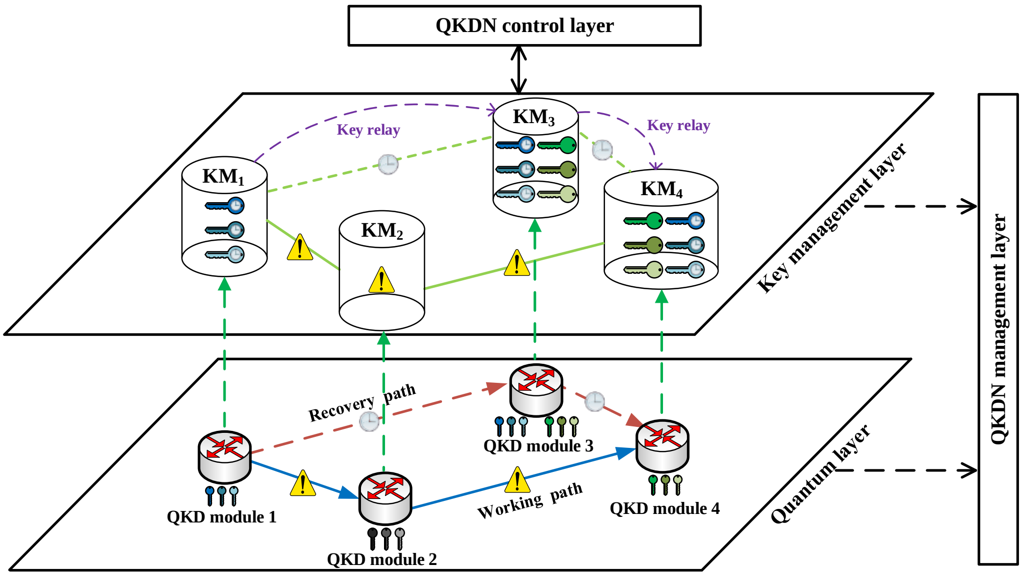

Figure 9 – Case 2.2 for QKDN resilience with recovery for multiple failures

Case 2.2) The working path through QKD modules 1, 2 and 4 supplies keys to cryptographic application A. If the QKD link from QKD module 1 to QKD module 2, and the link from QKD module 2 to QKD module 4 are impaired, the related QKD process could be interrupted. For the recovery of multiple failures, a QKD rerouting path could be searched for synchronized keys to recover the impaired key supply of application A, i.e., the QKD path which goes through QKD modules 1, 3 and 4. It can gradually recover the key supply with a single path searching in case of multiple failures. The time delay and other overheads caused by recovery should be considered.