**Abstract:** This document includes the output of Recommendation ITU-T Y.QKDN-rsfr “Framework of quantum key distribution network resilience”.

**Summary**

This TD is the output document for the draft Recommendation ITU-T Y.QKDN-rsfr “Framework of quantum key distribution network resilience” based on the following input contributions and the discussion during the Q16/13 meeting, 4 – 15 July 2022. As the discussion results, descriptions should be further improved.

|--------|-------------------------------------|-----------------------------------------------------------------------------------------------|-------|

- Proposal of contribution
  - This contribution proposes to clarify the uncertain aspects for QKDN resilience regarding the comments and suggestions during previous interim meetings as newly modified draft Recommendation ITU-T Y.QKDN-rsfr “Framework of quantum key distribution network resilience”.

**Source:** Editors  
**Title:** Draft Recommendation ITU-T Y.QKDN-rsfr: “Framework of quantum key distribution network resilience”

**Contact:**  
Xiaosong Yu  
Beijing University of Posts and Telecommunications.  
China  
Tel: +86-10-61198108  
E-mail: xiaosongyu@bupt.edu.cn

Yongli Zhao  
Beijing University of Posts and Telecommunications.  
China  
Tel: +86-10-61198108  
E-mail: yonglizhao@bupt.edu.cn

Yuhang Liu  
Beijing University of Posts and Telecommunications.  
China  
Tel: +86-15998440173  
E-mail: yuhangliu@bupt.edu.cn

Zhangchao Ma  
CAS Quantum Network Co., Ltd.  
China  
Tel: +86-10-83057625  
E-mail: mazhangchao@casquantumnet.com

**Geneva, 4-15 July 2022**
• Proposal of contribution
  – This contribution proposes to clarify the uncertain aspects of recovery for QKDN resilience with several updated diagrams regarding the comments and suggestions during previous interim meetings on draft Recommendation ITU-T Y.QKDN-rsfr “Framework of quantum key distribution network resilience”.

• Meeting result
  – The context should be further improved, including mainly two aspects. The first one is related to clarification of several terminology issues, such as “link and path recovery”, and also several statements, such as “reserve the QKD path”, etc. The second one is related to some duplication part in requirements, which needs to be improved.

• Editor’s note
  ✷ Clause 7: The position of control layer in diagrams should be clarified.
  ✷ Clause 8: The entities for reservation should be confirmed.

Attachments:

Annex A:

Draft Recommendation ITU-T Y.QKDN-rsfr

**Framework of quantum key distribution network resilience** Quantum key distribution networks – resilience framework

**Summary**

For **resilience in** quantum key distribution network (QKDN), **Y.QKDN-rsfr specifies framework of QKDN resilience**. This recommendation specifies describes the framework overview of QKDN resilience of resilience in QKDN including the conceptual models, scenarios and requirements of QKDN protection and recovery schemes. It also provides includes different typical use cases of QKDN resilience in the appendix and related requirements of resilience schemes supported by quantum layer, key management layer, and control and management layer, respectively.

**Keywords**

Quantum key distribution (QKD); QKD network (QKDN); QKDN resilience; framework; requirement.
# Table of Contents

1. Scope.......................................................................................................................... 5
2. References.................................................................................................................... 5
3. Terms and definitions .................................................................................................. 5
   3.1 Terms defined elsewhere ....................................................................................... 5
   3.2 Terms defined in this Recommendation ............................................................... 6
4. Abbreviations and acronyms ....................................................................................... 6
5. Conventions .................................................................................................................. 6
6. Overview of QKDN resilience ....................................................................................... 7
7. Scenarios of QKDN resilience .................................................................................... 8
   7.1 Protection of key supply in QKDN ......................................................................... 8
   7.2 Recovery of key supply in QKDN ......................................................................... 10
8. Requirements of 1+1 protection for QKDN resilience ................................................ 12
9. Requirements of 1:1 or 1:n protection for QKDN resilience ....................................... 13
10. Requirements of recovery for QKDN resilience ......................................................... 13
Appendix I Use cases of QKDN resilience ..................................................................... 15
Bibliography..................................................................................................................... 17
Draft Recommendation ITU-T Y.QKDN-rsfr

Quantum key distribution networks – resilience framework

1. Scope
This Recommendation illustrates the framework for resilience in QKDN resilience. It gives an overview on resilience in QKDN resilience with its related conceptual models, including protection and recovery. And it provides specifications requirements of QKDN multiple layers to support resilience in QKDN resilience as well as the use cases.

In particular, the recommendation includes:
- Overview of QKDN resilience in QKDN
- Scenarios of QKDN resilience in QKDN
- Requirements of 1+1 protection for QKDN resilience
- Requirements of 1:1 or 1:n protection for QKDN resilience
- Requirements of point to point recovery for QKDN resilience
- Appendix I: use cases of QKDN resilience
- Requirements of end to end recovery for QKDN resilience

2. References

< Others to be added>

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).

3.1.7 **Key request session recovery ratio** [ITU-T Y.3806]: the ratio of the numbers of recovered key request sessions to the total number of failed key request sessions.

3.1.8 **Wavelength reservation ratio** [ITU-T Y.3806]: the ratio of the reserved wavelength resources for recovery to the total of the allocated wavelength resources.

-TBD

3.2 **Terms defined in this Recommendation**

[Editor’s note: The necessity of definition for these general terms in QKDN needs to be confirmed.]

This chapter defines all the terms used in this recommendation.

3.2.1 **Resilience in QKDN**: The set of capabilities that allow a QKDN to protect or recover the QKD key supply within a threshold in the event of a QKD failure.

**NOTE** – In general, the resilience schemes will involve protection and recovery. For example, when resilience progress such as rerouting is performed, a percentage of the QKDN resources will be aggregated for the rerouting of impaired QKD key services.

3.2.2 **Failure in QKDN**: The fault cause of interrupted key supply persisted long enough to consider the ability of a QKD key service to perform a required function to be terminated.

-TBD

4 **Abbreviations and acronyms**

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

-TBD

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

The keywords “is not recommended” indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

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 resilience in QKDN

QKDN resilience provides the set of capabilities that allow a QKD to protect or recover the key supply process in the event of a QKD failure. This recommendation specifies the protection and recovery of key supply for QKDN resilience. It is necessary to be introduced into QKDN to guarantee stable running of QKDN and the continuous key supply. In this document, the framework of QKDN resilience and its requirements in QKDN are supported by multi-layer functions specified based on the functional requirements of QKD in [ITU-T Y.3801] and functional architecture of QKD in [ITU-T Y.3802]. The consideration on multi-layer QKDN resilience is based on the multi-layer functions specified in [ITU-T Y.3803] and [ITU-T Y.3804]. Expected effects on resilience in QKDN are based on descriptions in QoS related documents such as [ITU-T Y.3806]. In general, this recommendation is aimed to describe the resilience framework for QKDN resilience supported by functions and requirements of QKDN layers.

Keep QKD running in a robust status to provide the continuous protection of targeted traffic in the user network with stable key supply is an important issue in QKDNs. Failures in QKDN could be various such as classical channel’s interruption for key synchronization, quantum channel’s interruption for key generating, as well as QKD equipment’s breakdown, etc. The behaviours such as intentional eavesdropping could also cause the failures in QKDN operation. With these heterogeneous reasons that could not be distinguished from the view of network management, how to eliminate the unexpected influences is the main mission of resilience in QKDN. This recommendation focuses on how to protect the QKD from the unexpected key supply interruption and how to recover the network from this kind of anomalies effectively. With the hierarchical structure in QKD, the failures in each layer could also cause reactions in upper layers. And the immediate effects are reflected in key-supply anomalies, especially when a key supply interruption happens, the security of the services will be impaired. For example, if the communication on quantum channels is interrupted for reasons such as optical fibre cuts, key supply progress will be broken off caused by key-generation suspending. And the process in key management layer including key-relay going through the interrupted 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 QKD, it can be a systematic interruption that a key service cannot be provided. Thus, a framework of QKDN for resilience is needed for stable running of QKDN, it should be supported by multi-layer requirements to guarantee the continuous key supply.

This Recommendation will consider the following typical scenarios of resilience in QKDN resilience.

1) Resilience in QKDN supported by 1+1 protection;
2) QKDN resilience supported by 1:1 or 1:n protection;
3) QKDN resilience supported by point-to-point recovery;
4) Resilience in QKDN supported by end-to-end recovery.
In the following clauses, the recommendation specifies conceptual models of resilience in QKDN resilience. Use cases of resilience in QKDN resilience are included, and the resilience should also be supported by multiple layers with related requirements of QKDN resilience in quantum layer, key management layer, as well as control and management layer.

7 Scenarios of resilience in QKDN

![Figure 1 – A conceptual model of key-supply failure in QKDN](image)

As shown in Fig. 1, a conceptual model of key supply failure in QKDN is provided. A pair of keys generating is interrupted to be provided to the cryptographic application. The specific failure(s) could be located in quantum layer, as well as the key management layer. QKDN resilience manners including protection and recovery will be performed based on the specific scenarios key supply failure.

7.1 Protection of key supply in QKDN

[Editor's note: The position of control layer in diagrams should be clarified.]

QKDN protection aims to provide additional QKD services for stable key supply of specific cryptographic application QKDN through operations of multiple layers. These operations can guarantee the continuous key supply for stable guarantee of key supply in real time as when there occurs the event of key supply disruptions. Functional enhancement could be supported by multi-layer entities in QKDN. And the following expressions terms would be benefit to distinguish represent the status of QKD paths in the scenario of QKDN protection.

- **QKD working path**: a normal QKD path concatenated by QKD links connecting a pair of QKD nodes that normally provisioning keys concatenated by several point-to-point QKD links.
- **QKD protection path**: a pre-set QKD path connecting a pair of QKD nodes that pre-set to reserve the keys QKD service for QKD protection concatenated by selected point-to-point QKD links.
- **QKD protected path**: a QKD working path that matched with a QKD protection path. When the failure occurs over on the QKD protected path, its key provisioning would be replaced with the QKD protection path at in real time.

7.1.1 1+1 protection of key supply in QKDN

1+1 protection pre-sets the QKD protection path(s) for protection to guarantee the continuous key supply for the specific cryptographic application of QKDN. The reserved QKD service(s) over these paths for 1+1 protection are exclusively prepared reserved for the protected cryptographic application and cannot to overcome the key supply interruption in real time.

As shown in Fig. 2, a conceptual model of 1+1 key supply protection in QKDN is provided. The cryptographic application requires keys to guarantee the encrypted data transmitting. For the 1+1 protection scenario, the QKDN provides a twice the keys QKD protection path A-D-B required for the cryptographic application through an original QKD path and an additional QKD path for QKD...
protected path A\textsubscript{C}-B. If the original QKD path A\textsubscript{C}-B is impaired and related QKD process is interrupted, the supply of keys can be guaranteed by the additional QKD path A\textsubscript{D}-B in real time. This process could be achieved by deploying two physically separated pairs of QKD devices in the source and destination node for the additional QKD protection path. It can achieve a good effect on QKDN resilience, while the overhead of additional key consumption and the cost of additional QKD devices should be taken into consideration.

Figure 2 – A conceptual model of the 1+1 key-supply protection in QKDN

7.1.2 1:1 or 1:n protection of key supply in QKDN

1:1 or 1:n protection pre-sets the QKD protection path for protection to guarantee the continuous key supply for the specific set of cryptographic applications. QKD protected paths. The reserved QKD path QKD service over this path is exclusively prepared for the protected cryptographic applications and can overcome the key supply interruption in real time. Compared with 1+1 protection, the QKD links through the QKD protection path is can be also available for the other cryptographic applications that goes through them.

As shown in Fig. 3, a conceptual model of 1:1 key-supply protection in QKDN is provided. The cryptographic application requires keys to guarantee the encrypted data transmitting. For the 1:1 protection scenario, the QKD provides an alternative QKD protection path A-P-B is pre-set as the protection path. The QKD links A-P and P-B through the protection path work normally for its initial cryptographic application when there are no failures in the QKDN QKD protected path A\textsubscript{C}-B. When the QKD service over matched QKD protected path is impaired, this the alternative QKD protection path is enabled immediately to perform the key-relay process guaranteeing the original key provisioning supply of it for the influenced cryptographic application. Thus, the difference between 1:1 and 1+1 protection is that the pre-set QKD protection path for 1:1 protection is not enabled until the matched QKD protected path is impaired.

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

As shown in Fig. 4, a conceptual model of 1:n key-supply protection in QKDN is provided. Each cryptographic application in the application set requires keys to guarantee the encrypted data-
transmitting security. For the 1:n protection scheme, an alternative when the QKDN provides a QKD protection path A-P-B is pre-set as the protection path for n working QKD working paths. When one of the matched QKD protected paths is impaired with its QKD service, this alternative QKD protection path is enabled to perform the key-relay process guarantying the original key provisioning supply of it for the influenced cryptographic application.

**Note:** At the same time, this alternative the QKD protection path for 1:n protection can only be utilized for the protection of one single impaired QKD path at a time.

The 1:1 and 1:n protection schemes can achieve good effects on QKDN resilience, while the overhead of the pre-set additional QKD path, key consumption and the cost of additional QKD devices should be taken into consideration.

Figure 4 – A conceptual model of 1:n key-supply key-supply protection in QKDN

### 7.2 Recovery of key supply in QKDN

QKDN recovery aims to recover the impaired key supply for specific cryptographic application through operations of multiple layers. These operations search for the available QKD services that can gradually recover the key supply in a time period without reserving additional resources as there occurs the event of key supply disruptions. Functional enhancement could be supported by multi-layer entities in QKDN. Specifically, QKDN provides the function of re-routing to accomplish key-supply recovery as shown in Fig. 5.

- **QKD re-routing path:** A QKD path concatenated by QKD links that searched for key-supply recovery.

When there occurs the key-supply failure in QKDN, recovery maintains 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 additional operations including key-relay process. As a result, the interrupted key supply to cryptographic application can be gradually recovered. 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 6 – A conceptual model of recovery for single failure in QKDN**

As shown in Fig. 6, a conceptual model of recovery for single failure in QKDN is provided. For the scenario of recovery for single failure, when the specific QKD link A-B is impaired, the QKDN will search for a QKD re-routing path with sufficient resources to perform the key-relay process and replace the impaired key supply. It can gradually recover the key supply for QKDN resilience without the manners of reservation, while the overhead including time delay with re-routing should be taken into consideration.

**7.2.1 Point-to-point recovery of key supply in QKDN**

When there exists a failure in a specific QKD link, point-to-point recovery maintains the continuous key supply of this link through searching another QKD path between these adjacent QKD nodes for recovery. If the length of this QKD path exceeds one hop, it can replace the key provisioning of impaired QKD link with key-relay progress. As a result, the interrupted key supply to cryptographic application can be gradually recovered.

As shown in Fig. 5, a conceptual model of point-to-point recovery in QKDN is provided. The cryptographic application requires keys to guarantee the security of data transmission. For the point-
to-point recovery scheme, when the specific QKD link is impaired, the QKDN system will search for another QKD path to replace it, so that the keys can be re-supplied to the cryptographic application. It can achieve a good effect on QKDN resilience, while the overhead of the QKD path searching and keys consumption should be taken into consideration.

7.2.2 End-to-end recovery of key supply in QKDN

![Diagram of end-to-end recovery in QKDN](attachment:QKDN_recovery_diagram.png)

Figure 6 – A conceptual model of end-to-end recovery in QKDN

When there exist failures in a specific QKD path, end-to-end recovery maintains the continuous key supply of the impaired QKD path through searching another QKD path between the remote QKD nodes for recovery. And this QKD path can replace the impaired QKD links for key relay progress. As a result, the key supply to cryptographic application can be gradually recovered.

As shown in Fig. 6, a conceptual model of end-to-end recovery in QKDN is provided. The cryptographic application requires keys to guarantee the security of data transmission. For the end-to-end recovery scheme, when the original QKD path is impaired, the QKDN will search for another QKD path with sufficient resources to perform the key relay process and replace it, so that the keys can be re-supplied to the cryptographic application. It can achieve a good effect on QKDN resilience, while the overhead of QKD path searching should be taken into consideration.

8 Requirements of 1+1 protection for QKDN resilience

[Editor’s note: The entities for reservation should be confirmed.]

The 1+1 protection for resilience in QKDN requires functional support in multiple layers, including quantum layer, key management layer, and control and management layer.

8.1 Requirements of quantum layer for 1+1 protection

- QKDN is recommended to pre-set additional QKD paths as the QKD protection paths for 1+1 protection in quantum layer.
- The QKD protection path is recommended to have an equivalent QKD ability with the matched QKD protected path.

8.2 Requirements of key management layer for 1+1 protection

- QKDN is recommended to set KMA links and KSA links for the QKD protection paths in key management layer.
- QKDN is required to authenticate the reserved QKD-keys for 1+1 protection in key management layer.
Note: additional keys provided for 1+1 protection could be generate from multiple separate physical QKD paths, thus it could raise some of the insecurity factors that need authentication of these QKD paths.

- QKDN is required to reserve the keys generated by the QKD protection path that required for the exclusive use of the QKD protected path.

### 8.3 Requirements of QKDN-control and management layer for 1+1 protection
- QKDN is required to store data recording the matchup between QKD working paths and QKD protection paths in control and management layer.
- QKDN is required to monitor the status of key supplying and respond to the failed request in control and management layer.

### 9 Requirements of 1:1 or 1:n protection for QKDN resilience

The 1:1 or 1:n protection for resilience in QKDN requires functional support in multiple layers, including quantum layer, key management layer, and control and management layer.

#### 9.1 Requirements of quantum layer for 1:1 or 1:n protection
- 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.

#### 9.2 Requirements of key management layer for 1:1 or 1:n protection
- QKDN is recommended to reserve the keys generated by the over the protection path for the exclusive use of the QKD protected paths following a priority sequence.
  
  [Note: for the 1:n protection scenario, the QKD protected paths has the order of priority according to the user requirements.]

#### 9.3 Requirements of QKDN-control and management layer for 1:1 or 1:n protection
- QKDN is required to store data recording the matchup between QKD working paths and QKD protection paths in control and management layer.
- QKDN is required to monitor the status of key supplying and respond to the failed request in control and management layer.
- QKDN is recommended to formulate the priority policies for QKD protected paths according to the users’ requirements in control and management layer.

### 10 Requirements of point-to-point recovery for QKDN resilience

The point-to-point recovery requires functional support in multiple layers, including quantum layer, key management layer, and control and management layer.

#### 10.1 Requirements of quantum layer for point-to-point recovery
- QKDN is recommended to perform the point-to-point recovery for impaired QKD link without affecting the key supply of original key requests.
• QKDN can optionally search for the combination of multiple QKD paths (i.e., multi-path key provisioning) to recover the impaired point-to-point key provisioning to the cryptographic application.

10.2 Requirements of key management layer for point-to-point recovery

• The QKDN is recommended to search for the QKD re-routing path for point-to-point recovery within the toleration time of the cryptographic application related to the impaired QKD link.

10.3 Requirements of QKDN-control and management layer for point-to-point recovery

• QKDN is required to monitor the status of key supplying and respond to the failed request in control and management layer.
• QKDN can optionally record the operations of point-to-point recovery to update the QKD links’ information in control and management layer.
• QKDN is recommended to perform the recovery for single failure or multiple failures based on the policies in QKDN control and management layer.

11 Requirements of end-to-end recovery for QKDN resilience

The end-to-end recovery requires functional support in multiple layers, including quantum layer, key management layer, and control and management layer.

11.1 Requirements of quantum layer for end-to-end recovery

• QKDN is recommended to perform the end-to-end recovery for impaired QKD links without affecting the key supply of original key requests.
• QKDN can optionally search for the combination of multiple QKD paths (i.e., multi-path key provisioning) to recover the impaired end-to-end key provisioning to the cryptographic application.

11.2 Requirements of key management layer for end-to-end recovery

• The QKDN is recommended to search the QKD path for end-to-end recovery within the toleration time of the cryptographic application related to the impaired QKD links.

11.3 Requirements of QKDN control and management layer for end-to-end recovery

• QKDN is required to monitor the status of key supplying and respond to the failed request in control and management layer.
• QKDN can optionally record the operations of end-to-end recovery to update the QKD links’ information in control and management layer.
Appendix I

Use cases of QKDN resilience in QKDN

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

How to recover the QKDN resources under a QKD impairment is an important issue to be solved for QKDN resilience in QKDN. With multi-layer functional requirements and architecture described in Y.3800 to 3804, the QKDN resilience in QKDN requires collaborative operations among QKDN multiple layers. Figures 7-10 show several conceptual models of typical resilience cases use cases in of QKDN resilience as well as corresponding operations with the support of QKDN multiple layers.

Use cases of QKDN resilience in QKDN including 1+1 protection, 1:1 or 1:n protection, point-to-point recovery, and end-to-end and recovery are described in this recommendation appendix.

I.1 Use case of 1+1 protection in QKDN

![Diagram of 1+1 protection in QKDN]

Figure 7-8 – Case 1 of QKDN resilience in QKDN with 1+1 protection

Case 1) The keys are provided with key relay through QKD module 1, QKD module 2 and QKD module 4 to the cryptographic application guarantying the encrypted data transmitting of encryption service A-A. If the QKD link from QKD module 1 to QKD module 2 is impaired, the related QKD process could be interrupted and the transmission of encrypted data cannot be guaranteed. For the 1+1 protection scenario, the QKDN provides additional keys required by the cryptographic application through key relay over additional QKD protection path, which goes through QKD module 1, QKD module 3 and QKD module 4. Thus, if the QKD protected path is impaired, the supply of keys can be guaranteed by the QKD protection path. For QKDN, such behaviour The 1+1 protection of providing twice the keys required by the cryptographic application can achieve a good effect on QKDN resilience, while the waste expense of additional key resource and the cost of additional QKD devices should be taken into consideration.
I.2 Use case of 1:1 or 1:n protection in QKDN

Figure 8–9 – Case 2 of QKDN resilience in QKDN with 1:1 or 1:n protection

Case 2) The keys are provided with key relay through QKD module 1, QKD module 2 and QKD module 4 to cryptographic application guarantying the encrypted data transmitting of encryption service A. In order to avoid the interruption of the QKD process caused by the failure of specific QKD path, we could respectively adopt 1:1 or 1:n protection scheme as follows:

For the 1:1 protection scenario, an additional QKD path (i.e., the path goes through QKD module 1, QKD module 3 and QKD module 4) is pre-set as the QKD protection path. The QKD links on this protection path is reserved for the QKD protected path. When the QKD protected path is impaired, leading to the interruption of encryption service A, the QKD protection path is enabled immediately to perform the key-relay process to guarantee the key provisioning of the influenced encryption service A.

For the 1:n protection scenario, the additional QKD path is pre-set as the QKD protection path for n QKD working paths. Thus, when one of the QKD protected paths is impaired, the QKD protection path is enabled to perform the key-relay process to guarantee the key provisioning of the influenced encryption service A. At the same time, the QKD protection path can only be utilized for the protection of one impaired QKD path.

I.3 Use cases of point-to-point recovery in QKDN
Figure 9-10 – Case 3.1 of QKDN resilience in QKDN with point-to-point recovery for single failure

Case 3.1) The keys are provided between QKD module 1 and QKD module 2 to cryptographic application guarantying the encrypted data transmitting of encryption service A-A. If the QKD link from QKD module 1 to QKD module 2 is impaired, the related QKD process could be interrupted and the transmission of encrypted data cannot be guaranteed. For the point-to-point recovery scenario of single failure, when the failure occurs, a QKD rerouting path will be constructed for key relay to recover the impaired key supply of service A, such as the QKD path which goes through QKD module 1, QKD module 3, QKD module 4, and finally QKD module 2. The time delay and other overheads caused by the point-to-point recovery should be considered.

I.4 Use case of end-to-end recovery in QKDN

Figure 10-11 – Case 4.3.2 of QKDN resilience in QKDN with end-to-end recovery for multiple failures

Case 4.3.2) The keys are provided with key relay through QKD module 1, QKD module 2 and QKD module 4 to cryptographic application guarantying the encrypted data transmitting of encryption service A. If the QKD link from QKD module 1 to QKD module 2, or and the link from QKD module 2 to QKD module 4 are impaired, the related QKD process could be interrupted and the transmission of encrypted data cannot be guaranteed. For the end-to-end recovery scenario of multiple failures, when the failures occur, a QKD rerouting path will be constructed for key relay to recover the impaired key supply of service A, such as the QKD path which goes through QKD module 1, QKD module 3 and QKD module 4. The time delay and other overheads caused by end-to-end recovery should be considered.

Bibliography