International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1714

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Quantum communication – Security design for QKDN

Key combination and confidential key supply for quantum key distribution networks

Recommendation ITU-T X.1714

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	**X.1712–X.1719**
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1714

Key combination and confidential key supply for quantum key distribution networks

Summary

Recommendation ITU-T X.1714 describes key combination methods for quantum key distribution network (QKDN) and specifies security requirements for both the key combination and the key supply from QKDN to cryptographic applications.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1714	2020-10-29	17	11.1002/1000/14453

Keywords

Key combination, key supply, QKD, QKD network, quantum key distribution.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1714

Key combination and confidential key supply for quantum key distribution networks

1 Scope

This Recommendation describes key combination methods for quantum key distribution network (QKDN) and specifies security requirements for both the key combination and the key supply from QKDN to cryptographic applications.

In particular, this Recommendation addresses the following points:

– the security of the combination of keys exchanged through a QKDN and keys exchanged through other key exchange methods;

– the security of the key supply from a QKDN to cryptographic applications.

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 Y.3800] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution*, plus Corrigendum 1 (2020).

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture of quantum key distribution networks.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 key management [ITU-T Y.3800]: All activities performed on keys during their life cycle starting from their reception from the quantum layer, storage, formatting, relay, synchronization, authentication, to supply to a cryptographic application and deletion or preservation depending on the key management policy.

3.1.2 key management agent (KMA) [ITU-T Y.3802]: A functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node).

NOTE – KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats and stores them. It also relays keys through key management agent (KMA) links.

3.1.3 key supply [ITU-T Y.3800]: A function providing keys to cryptographic applications.

3.1.4 key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE – Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

3.1.5 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.

3.1.6 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.

3.1.7 quantum key distribution node (QKD node) [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

KMA Key Management Agent

KSA Key Supply Agent

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

SIM Subscriber Identity Module

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

6 Introduction

Key combination is a method to combine multiple keys generated by different key exchange methods. For example, in public key cryptography, key combination is useful when the key consumer does not want to rely on a single key exchange method or wants to use a recent key exchange method with a security that has not been fully demonstrated yet (e.g., post-quantum public key cryptographic algorithms). The key resulting from an appropriate key combination can be secure as long as one of the keys used as inputs for this combination remains secure [b-Giacon], [b-Bindel]. Therefore, key combination may be beneficial from the viewpoint of migration towards the adoption of quantum key distribution networks (QKDNs) into network infrastructures.

Quantum key distribution (QKD) is a cryptographic technology which allows the sharing of symmetric random bit strings (key) between two remote parties. The confidentiality of the key provided by QKD protocols can be proven based on quantum information theory. Linking an ensemble of pairs of QKD modules with key relay techniques is the building block of QKD networks (QKDNs). General aspects, functions and structures of the QKDN are described in [ITU-T Y.3800].

A key combination can be applied to keys established by quantum key distribution (QKD) and its network (QKDN).

A key combination that preserves the confidentiality guaranteed by QKD provides a secure cryptographic key. However, the security of the key combination should be carefully analysed since the confidentiality of QKD is based on quantum physics and statistical properties, whereas in most of the current cryptographic technologies, including key combinations, the security is based on computational complexity.

Furthermore, in QKDNs, quantum physics guarantees the confidentiality of the key exchange between two QKD modules. However, the confidentiality of the key supply between these QKD modules and the cryptographic applications consuming its keys does not rely on quantum physics. In order to provide an end-to-end confidentiality on keys, the security of keys supplied by QKD needs to be specified.

This Recommendation describes the concept of the key combination method in clause 7, and specifies some security requirements of key combination methods in clause 8. The security requirements for key supply between QKDNs and cryptographic applications are covered in clause 9.

7 Key combination methods for QKDN

This clause defines a key combination for QKDN. Figure 1 shows a general description of the key combination considered in this Recommendation. It consists of a key combiner which transforms two or more input keys supplied by different key exchange methods into a combined key. One of the input keys is supplied by a QKD-based key exchange. When the key combiner is located outside the QKDN and used in the service layer (see [ITU-T Y.3800] for a layer structure and basic functions of QKDN), the QKD-based key exchange is a key exchange performed by the QKDN. When the key combiner is in the QKDN, the QKD-based key exchange is a key exchange between QKD modules with or without key relays. The other input keys can be provided by any kind of method allowing the exchange of symmetric keys between two nodes, including cryptographic means and physical means (e.g., subscriber identity module (SIM) card). In this Recommendation, the input key provided by the QKD-based key exchange is referred to as K_{QKD}, and the input keys provided by the other key exchanges are referred to as K_1, K_2, ... The key resulting from the key combination, or combined key, is referred to as K_C. K_C is sent to cryptographic applications.

The key combiner can output a combined key, even if the QKD-based key exchange cannot supply a key. In this case, the key combiner can use a pre-shared value K_{ps}. Then, the security of the combined key K_C is guaranteed either by K_{ps} or by the other keys (K_1, K_2, ...).

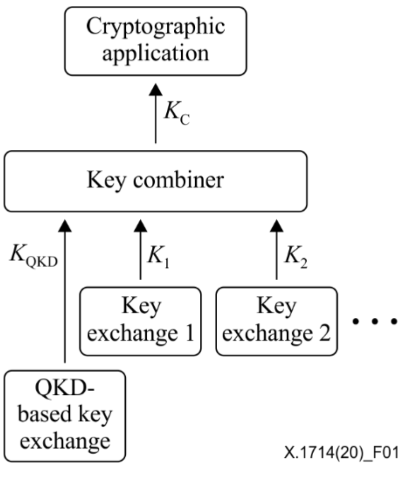

Figure 1 – Key combination method for QKDN

NOTE – Information about possible locations of a key combiner is given in [ITU-T Y.3802] and [ITU-T Y.3803].

8 Security requirements for key combination methods

This clause describes the security requirements for the key combination methods for QKDN. The requirements depend on where the key combiner is located.

If the key combiner is located outside the QKDN and is used as a cryptographic application, the requirements fully depend on the policy of the user of the application. Specification of the security requirements in this case is outside the scope of this Recommendation.

The security requirements for the key combiners in the QKDN are listed below:

Req.1 If K_{QKD} is available and used as the input key, the key combiner is required to output K_{C} that maintains the confidentiality of K_{QKD} in a statistical sense.

To satisfy Req.1, requirements Req.2 to Req.4 are also needed:

Req.2 The key length of K_{C} is required to be not longer than the key length of K_{QKD}.

Req.3 K_{QKD} and the other input keys are required to be statistically independent.

Req.4 The input keys from the other key exchange methods (K_1, K_2, ...) are required to have a discrepancy rate lower than a value defined in the security policy of the QKDN.

Since confidentiality of the key supplied from QKD is based on its statistical property, confidentiality of the combined key from the key combiner should also be evaluated in the same manner. An example of the key combination method satisfying Req.1 is an exclusive or (XOR) operation of multiple independent input keys with the same length.

NOTE 1 – "discrepancy" in Req.4 means that the exchanged key values between the nodes are not identical. A low discrepancy rate is usually a reasonable assumption for computational algorithm-based cryptography or some physical cryptographic means such as SIM cards. However, if this discrepancy rate is not sufficiently low, the discrepancy of the other keys may degrade the security of the combined key compared to the security of the input key supplied from the QKD-based key exchange. In this case, the discrepancy probability of keys needs to be bounded under a threshold which is defined in security policies of QKDNs and cryptographic applications.

One additional security requirement for the key combiners located in the functional element that supplies keys to cryptographic applications is listed below:

NOTE 2 – This functional element that supplies keys to cryptographic applications is called key supply agent (KSA) and is defined in [ITU-T Y.3802] and [ITU-T Y.3803].

Req.5 If the pre-shared value K_{ps}, is used as the input key, instead of K_{QKD}, the key combiner is required to announce the unavailability of the key from the QKD-based key exchange to the cryptographic application.

NOTE 3 – When K_{ps} is used as the input key, the confidentiality of the combined key K_{C}, is guaranteed either by K_{ps} or by the other keys (K_1, K_2, ...).

9 Security requirements for key supply between QKDNs and cryptographic applications

This clause describes the security requirements for the key supply between a QKDN and cryptographic applications.

Req.6 The QKDN and the cryptographic applications connected to it are recommended to have the capability to secure the key supply.

Req.7 The QKDN and the cryptographic applications connected to it are recommended to encrypt the supplied keys by using symmetric key encryption schemes.

Req.8 The QKDN and the cryptographic applications connected to it are recommended to use symmetric key encryption algorithms that are considered as robust against attacks performed with a quantum computer.

NOTE – At the time of the writing of this Recommendation, symmetric key encryption algorithms considered as robust against quantum computing offered at least a 128-bit security level in the presence of quantum computers able to halve the symmetric key space, amounting to the use of at least 256-bit symmetric keys.

Bibliography

[b-ETSI GR QKD 007] ETSI GR QKD 007 V1.1.1 (2018), *Quantum Key Distribution (QKD);Vocabulary*.
<https://www.etsi.org/deliver/etsi_gr/QKD/001_099/007/01.01.01_60/gr_qkd007v010101p.pdf>

[b-Bindel] Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., and Stebila, D. (2019), *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange*,
<https://eprint.iacr.org/2018/903.pdf>

[b-Giacon] Giacon, F., Heuer, F., and Poettering B. (2018), *KEM Combiners*,
<https://eprint.iacr.org/2018/024.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021