International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1702

(11/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Quantum communication

Quantum noise random number generator architecture

Recommendation ITU-T X.1702

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	**X.1700–X.1729**

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

Recommendation ITU-T X.1702

Quantum noise random number generator architecture

Summary

Recommendation ITU-T X.1702 defines a generic functional architecture of a quantum entropy source, a common method to estimate and validate the entropy of a noise source under evaluation, and a common method to specify randomness extractors when they are part of the implemented system.

In contrast to the causal nature of classical physics, the inherently probabilistic nature of quantum physics is particularly suited to implement noise sources with an entropy that can be estimated based on information theory. However, there are currently no existing standards that explicitly distinguish between noise sources based on quantum physics and classical physics. This Recommendation is an add-on to existing noise or entropy source standards that allow specification of the noise source under evaluation based on quantum physics.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1702	2019-11-13	17	11.1002/1000/14095

Keywords

Quantum entropy source, random bit generator, random number generator.

---

* 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

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	General discussion	3
7	Functional architecture of quantum entropy sources	3
8	Entropy estimation	5
9	Entropy assessment	5
10	Randomness extractors (optional)	5
Bibliography		7

Introduction

The creation of a series of random numbers (or, bits) is a matter of concern for the security community. Random numbers are important in a wide variety of security services – i.e., random values used for key establishment protocols, random keys and initial values [b-ISO/IEC 18031] for encryption, random keys for authentication and digital signature, etc. The security of cryptographic systems using random bits relies on the entropy of those random bits. Random bit sequences are mainly characterized by two properties: their uniformity and their unpredictability. Uniformity of random bit sequences can be generated using several physical or non-physical techniques. Unpredictability of random bit sequences is much more complicated to achieve. Quantum physics allows the generation of unpredictable random bit sequences because of its probabilistic nature. Hence, the security community needs a functional architecture for generating and testing series of random numbers generated by non-deterministic random bit generators (NRBG) exploiting quantum physics.

Different applications have different requirements for random numbers. In some applications, random bit sequences with an imperfect entropy are sufficient to meet the requirements. However, in some cryptographic applications, such as bit commitment, encryption, etc., it is difficult to ensure the security of these applications without using random numbers that are very close to uniform distribution [b-Herrero] and [b-Ma2016].

To increase the entropy of random number sequences, these sequences are post-processed by randomness extractors. The function of a randomness extractor is to transform a raw random bit flow from an entropy source into random number sequences that have an entropy very close to 1 [b-Herrero] and [b-Ma2013]. External attacks, for example, side-channel attacks and fault induced attacks, should be considered in the construction of NRBGs. In existing standards, such as [b-BSI AIS20/AIS31], algorithmic post-processing (randomness extractor) is generally used against external attacks, but those standards only consider the classical adversary cases where an adversary only attacks a NRBG with classical means. Quantum means are more powerful than classical means when attacking a NRBG and not all classical randomness extractors are quantum-proof extractors (i.e., secure against quantum attacks) [b-Ben-Aroya] and [b-Gavinsky]. So far, two randomness extractors, Trevisan's extractor [b-Trevisan] and [b-Ma2013] as well as two universal hashing [b-König]and [b-Ma2013], have proven to be secure against quantum attacks.

This Recommendation specifies a functional architecture for random number generation based on quantum phenomena. Also, this Recommendation aims at making a clear distinction between NRBGs based on classical physics and those based on quantum physics.

Recommendation ITU-T X.1702

Quantum noise random number generator architecture

1 Scope

This Recommendation provides a set of recommendations for a specific evaluation of entropy sources to distinguish non-quantum physical entropy sources from quantum physical entropy sources. It also provides the following specification regarding quantum physical entropy sources:

– a description of quantum entropy sources using quantum physics formalism and a generic functional architecture for quantum entropy sources;

– a common way to estimate the entropy of quantum entropy sources;

– a verification of the entropy generated by the source depending on its subclass;

– a common way to specify randomness extractors (when applicable).

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed (peer-entity authentication). The corroboration that the source of data received is as claimed (data origin authentication).

3.1.2 digital signature [b-ITU-T X.800]: Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.

3.1.3 entropy source [b-NIST SP 800-90B]: The combination of a noise source, health tests, and an optional conditioning component that produces random bit strings to be used by a random bit generator.

3.1.4 initial value(initialisation value) [b-ISO/IEC 18031]: Value used in defining the starting point of a cryptographic algorithm (e.g., a hash-function or an encryption algorithm).

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 nonce: A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness, thus detecting and protecting against replay attacks.

NOTE – Definition based on [b-IETF RFC 4949].

3.2.2 non-physical entropy sources: An entropy source that does not use dedicated hardware but uses system resources (RAM content, thread number etc.) or the interaction of the user (time between keystrokes, etc.).

NOTE – This definition is identical to the definition of 'non-physical non-deterministic random bit generator' given in [b-NIST SP 800-90B].

3.2.3 physical entropy sources: An entropy source that uses dedicated hardware or uses a physical experiment (noisy diode(s), oscillators, event sampling like radioactive decay, etc.).

NOTE – This definition is identical to the definition of 'physical non-deterministic random bit generator' given in [b-NIST SP 800-90B].

3.2.4 QES1: A subclass of quantum entropy sources that will assess a given minimum entropy amount by measuring the implementation imperfections and verifying that they are within defined acceptable value ranges.

3.2.5 QES2: A subclass of quantum entropy sources that will assess their generated entropy amount by measuring signatures of the quantum process.

3.2.6 quantum entropy source (QES): An entropy source based on at least one quantum phenomenon.

NOTE – Examples of quantum phenomena include quantum state superposition, quantum state entanglement, Heisenberg uncertainty, quantum tunnelling, spontaneous emission or radioactive decay.

3.2.7 signature of a quantum process: A set of measurable statistical properties that are characteristic of a given quantum process according to some assumptions provided in the description, and that permits quantification of this process' impact on the measurement outputs in a manner that enables a direct or indirect estimation of the minimum amount of entropy coming solely from the quantum process. For example, one signature of quantum entanglement is the violation of Bell inequalities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DRBG Deterministic Random Bit Generator

NRBG Non-deterministic Random Bit Generator

QES Quantum Entropy Source

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 Recommendation 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 Recommendation 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 General discussion

Standards are compulsory in many security use-cases. There are at least three standards addressing the construction and evaluation of non-deterministic random bit generators (NRBGs): [b-NIST SP 800-90B], [b-BSI AIS20/AIS31] and [b-ISO/IEC 18031]. None of the three standards make any distinctions on the origin of the noise source.

However, within physical noise sources, quantum noise sources (i.e., the noise sources relying on a quantum effect), can be established as uniform thanks to quantum information theory. Indeed, the entropy of these sources can be calculated based on an understanding of the quantum process. This is not the case of non-quantum physical noise sources which employ causal processes hidden behind complexity; they can only be described as unpredictable after making assumptions of an adversary's lack of knowledge.

NOTE – The expression 'quantum process' is used to describe the whole method of exploitation of the quantum effect to generate quantum noise.

The entropy estimation of quantum noise sources is based on ideal models that are difficult to implement perfectly. This means that in most cases, the entropy of a quantum noise source is partly due to the relevant quantum process and some additional physical noise coming from implementation imperfections. Nevertheless, it is possible for most quantum noise sources to estimate the entropy solely due to the relevant quantum process.

Quantum entropy sources can be classified in two subclasses depending on their means of entropy estimation. One subclass of quantum entropy source will assess a given minimum entropy amount by measuring the implementation imperfections and verifying that they are within defined acceptable value ranges. This subclass of quantum entropy sources (QESs) is called QES1. Another subclass of QESs, called QES2, will directly assess their entropy amount by measuring signatures of the quantum process. Then, in both cases, by using an appropriate randomness extractor, it is possible to create an output whose entropy arises solely from the considered quantum process.

The characteristics cited above make quantum entropy sources clearly different from non-quantum entropy sources. Therefore, this Recommendation specifies a method of distinguishing quantum entropy sources from other physical and non-physical entropy sources. However, this method needs to be compatible with existing evaluation standards, such as [b-NIST SP 800-90B], [b-BSI AIS20/AIS31] and [b-ISO/IEC 18031]. For this purpose, this Recommendation defines a generic functional architecture that can be used by different types of quantum entropy sources to describe the expected entropy as requested in these evaluation standards for an entropy source.

7 Functional architecture of quantum entropy sources

As proposed in [b-Ma2013], a quantum process to generate quantum noise can be decomposed in two steps: a quantum state preparation and a quantum state measurement. Therefore, the generation of raw data by a digital quantum noise source can be described in three, or optionally four functional steps as depicted in Figure 7-1. Each step is associated with one functional module as follows:

1) quantum state preparation: The quantum state can be optical or non-optical and either remain the same or be different in each iteration. The preparation can be active or passive;

2) quantum state measurement: Applying a measurement basis to the propagated state or the state derived from the quantum state preparation. This measurement basis can either remain the same or be different from one measurement to another;

   NOTE 1 – The combination of the 'quantum state preparation' module and the 'quantum state measurement' module composes an analogue quantum noise source.

3) raw data acquisition: This step is to generate raw data from quantum state measurement results. A digitization step is needed if the quantum state measurement results are analogue. The raw data acquisition module outputs the raw data that will be used to generate the digital quantum noise source output;

4) post-processing (optional): In some cases, the raw data might be post-processed before being output as entropy source output. One of the possible reasons of using post-processing is to increase the entropy content of each bit of the entropy source output.

Depending on the number of functional steps used for the description of the quantum entropy source, this entropy source can output either the raw data generated by the 'raw data acquisition' step, or the output from the 'post-processing' step.

For the assessment of the entropy generated by the quantum process and carried by the raw data, there is also a three-step process as depicted in Figure 7-1:

1) source parameter monitoring: The source parameters are acquired by this function to be used as inputs for the verification of the entropy of the raw data;

2) raw data acquisition: The source parameters are digitized and added in the flow of raw data. These source parameters will not be used to generate the output flow of the entropy source but to verify its entropy;

NOTE 2 – The raw data is composed of the bit sequence ('measurement result') and additional digital values ('parameter value', e.g., temperature, voltage, tampering attempts etc.) generated by the entropy source.

3) entropy verification: The raw data will be processed in order to verify if the entropy generated by the digital quantum noise source is at least higher than the minimum entropy amount specified (see clause 9) by the submitter. If this is not the case, an error message will be generated by the 'entropy verification' module and output from the quantum entropy source.

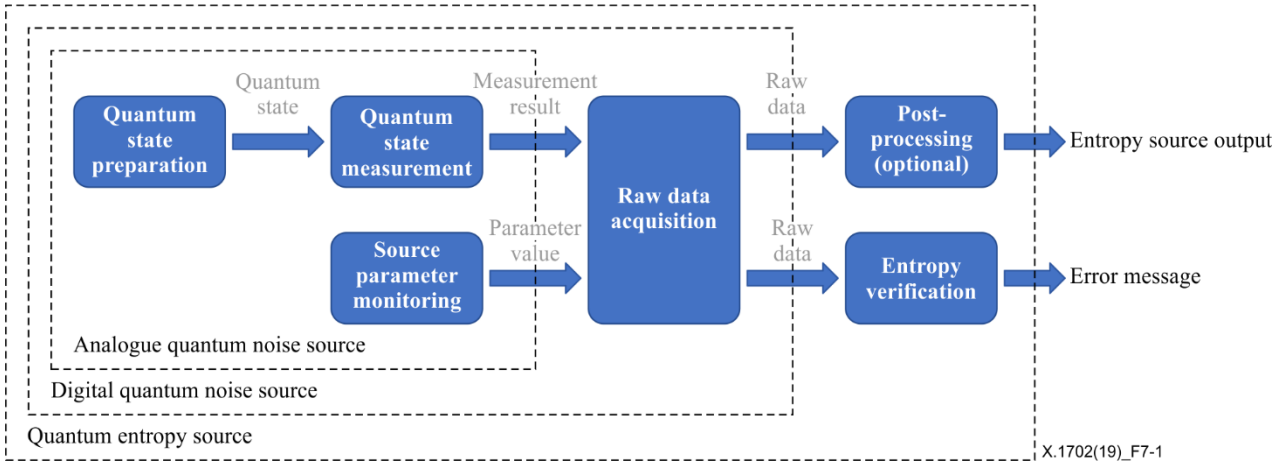

Figure 7-1 – Functional architecture of a quantum entropy source

The description of a quantum entropy source under evaluation is required to be based on the functional architecture presented in Figure 7-1. The description of the quantum state preparation and measurement modules is required to rely on quantum formalism.

Furthermore, the description of a quantum entropy source is required to include the definitions of the conditions (e.g., environmental constraints) under which this description remains valid.

In the case of QES1 sources, these conditions are required to include at least:

– the noise arising from implementation imperfections; and

– the range over which the value of this noise can vary.

In the case of QES2 sources, these conditions are required to include at least:

– the signature(s) of the quantum process (as defined in clause 3.2.7); and

– their acceptance range used to assess the entropy of the quantum source under evaluation and to ensure the continued working of the components of the system.

8 Entropy estimation

A method of estimation of the entropy generated by the quantum entropy source under evaluation is required to be based on the description (see clause 7) of this source. This estimation is recommended to be based on quantum information theory or other approved methods related to quantum physics.

NOTE 1 – Several types of entropy exist, such as Shannon, Von Neuman and min entropy.

NOTE 2 – The entropy of quantum states can be calculated from its density matrix [b-Bengtsson].

This entropy estimation is required to quantify the minimum amount of entropy generated by the quantum entropy source coming solely from the quantum process.

In the case where the submitter does not use a post-processing module in their quantum entropy source, this amount of entropy is required to be used by the submitter for their entropy estimation.

9 Entropy assessment

Entropy assessment consists in verifying that the conditions defined in the quantum entropy source description and used in the entropy estimation are in acceptable ranges to guarantee that the generated entropy value is larger than the estimated entropy value.

A source parameter monitoring function (see clause 7) is required to monitor the conditions under which the raw data is generated by the digital entropy source as specified in clause 7.

An entropy verification is required to verify that those conditions are valid based on the description (see clause 7) made by the submitter.

In the case of QES1 entropy sources, the monitoring function is required to monitor all the conditions listed in the description of the quantum entropy source that impact the entropy value of this source (e.g., noise arising from implementation imperfections and external conditions).

In the case of QES2 entropy sources, the monitoring function is required to estimate the signature(s) of the quantum process (as defined in clause 3.2.7) and to compare them with their acceptance ranges defined in the description in order to assess the entropy of the source and to ensure components of the system are operating within acceptable parameters where required by the description.

10 Randomness extractors (optional)

As shown in the functional architecture described in Figure 7-1, a post-processing module can optionally be used to increase the entropy per bit of the quantum entropy source output. Such post-processing modules are also called randomness extractors.

This clause focuses on the case where the submitter wants to increase the entropy per bit of their source to be secured against quantum attacks. In this specific case, the randomness extractor is required to be a quantum-proof extractor. The minimum amount of entropy at the output of this quantum-proof randomness extractor is required to be used by the submitter as submitter entropy estimation.

NOTE 1 – At the time of drafting this Recommendation, only two known quantum-proof randomness extractors existed: Trevisan's extractor [b-Trevisan], [b-Ma2013] and a 2-universal hashing [b-König], [b-Ma2013].

NOTE 2 – There are several methods to increase or decrease the entropy of a bit stream without taking into account quantum attacks. Those methods are out of the scope of this Recommendation. Some of these are recommended in other recommendations for random number generators (RNGs) as for example [b-NIST SP 800-90B], [b-BSI AIS20/AIS31] and [b-ISO/IEC 18031].

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1911), *Security architecture for Open Systems Interconnection for CCITT applications.*

[b-Ben-Aroya] Ben-Aroya, A., and A. Ta-Shma, (2012), *Better short-seed quantum proof extractors*, Theor. Comput. Sci. 419, 17–25.

[b-Bengtsson] Bengtsson, I., & Życzkowski, K. (2017), *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge university press.

[b-BSI AIS20/AIS31] BSI AIS20/AIS31 (2011), *A proposal for: Functionality classes for random number generators*.

[b-Gavinsky] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, R. de Wolf, (2008), *Exponential separations for one-way quantum communication complexity, with applications to cryptography*, SIAM Journal on Computing 38 (5) 1695–1708.

[b-Herrero] M. Herrero-Collantes and J. C. Garcia-Escartin, (2017), *Quantum Random Number Generators.* REVIEWS OF MODERN PHYSICS, 89.

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet Security Glossary, Version 2.*

[b-ISO/IEC 18031] ISO/IEC 18031:2011 (2011), *Information technology – Security techniques – Random bit generation*.

[b-König] König, R., and R. Renner (2011), *Sampling of Min-Entropy Relative to Quantum Knowledge*, IEEE Trans. Inf. Theory 57, 4760–4787.

[b-Ma2013] Ma, X., Xu, F., Tan, X., Qi, B.and Lo, H-K. (2013), *Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction*, Phys. Rev. A, Vol. 87, 062327.

[b-Ma2016] X. F. Ma, X. Yuan, Z. Cao, B. Qi and Z. Zhang (2016), *Quantum random number generation. npj Quantum Information*.

[b-NIST SP 800-90B] NIST SP 800-90B (2018), *Recommendation for the Entropy Sources Used for Random Bit Generation*.

[b-Trevisan] Trevisan, L., (2001), *Extractors and pseudorandom generators*, J.ACM 48, pg. 860–879.

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, 2020