International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1811

(04/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

IMT-2020 Security

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

Recommendation ITU-T X.1811

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
IMT-2020 SECURITY	**X.1800–X.1819**

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

Recommendation ITU-T X.1811

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

Summary

Recommendation ITU-T X.1811 identifies threats raised by quantum computing to International Mobile Telecommunications-2020 (IMT-2020) systems through assessing the security strength of currently used cryptographic algorithms. This Recommendation briefly reviews quantum safe algorithms, including both symmetric and asymmetric types, and provides guidelines for applying quantum safe algorithms in IMT-2020 systems.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1811	2021-04-30	17	11.1002/1000/14454

Keywords

5G system, asymmetric algorithm, IMT-2020 system, quantum computer, quantum-safe algorithm, symmetric algorithm.

* 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 received notice of intellectual property, protected by patents/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The International Mobile Telecommunications-2020 (IMT-2020) system promises to support a wide range of services with diverse performance requirements in order to form a fully connected society. To achieve this challenging goal, a number of innovative technologies have been developed in the IMT-2020 system, such as network slicing, the software-defined network, virtualized network function and central unit/distributed unit (CU/DU) separation. Security measures are fundamental to ensuring the normal operation of the IMT-2020 system. Besides the use of symmetric cryptographic algorithms, those that are asymmetric, have been deployed in the IMT-2020 system.

A large-scale quantum computer raises security concerns to current widely used symmetric and asymmetric cryptographic algorithms. The latter no longer provide security in the quantum-computing era. Furthermore, symmetric cryptographic algorithms have to double their key lengths to resist quantum-computing attacks. For this, deployment of quantum-safe cryptographic algorithms is highly desirable in the IMT-2020 system.

In this Recommendation, the IMT-2020 system and its security architecture are briefly surveyed. The threats to IMT-2020 systems due to quantum computers are assessed. Quantum-safe algorithms are briefly reviewed, but their details are not specified in this Recommendation. Security guidelines will be included in a high-level Recommendation to adapt quantum-safe algorithms to IMT-2020 systems. This Recommendation is intended to provide the guidelines for the application of quantum-safe symmetric and asymmetric algorithms to the IMT-2020 system, as well as the alignment of security levels between quantum-safe symmetric and asymmetric algorithms.

Recommendation ITU-T X.1811

Security guidelines for applying quantum-safe algorithms in IMT-2020 systems

1 Scope

This Recommendation covers:

– an introduction to the security architecture of International Mobile Telecommunications-2020 (IMT-2020) systems;

– a security assessment of IMT-2020 systems when commercial quantum computers are available;

– a specification of the usage of quantum-safe algorithms in IMT-2020 systems.

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.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T Y.2014]: A property by which the correct identity of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.

3.1.2 authentication protocol [b-ITU-T X.1254]: A defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.1.3 authorization [b-ISO 7498-2]: The granting of rights, which includes the granting of access based on access rights..

3.1.4 availability [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.6 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.7 data integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 privacy [ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.9 key hierarchy [b-ITU X.1196]: A tree structure that represents the relationship of different keys. In a key hierarchy, a node represents a key used to derive the keys represented by the descendent nodes. A key can only have one precedent, but may have multiple descendent nodes.

3.1.10 network function virtualization; NFV [b-ISO/IEC TR 22417]: Technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

4G	fourth Generation
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard-Cipher Blocker Chaining
AES-GCM	Advanced Encryption Standard-Galois Counter Mode
AES-GMAC	Advanced Encryption Standard-Galois Message Authentication Code
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility management Function
API	Application Programming Interface
ARPF	Authentication credential Repository and Processing Function
AS	Access Stratum
AUSF	Authentication Server Function
AV	Authentication Vector
CEK	Content Encryption Key
CM	Configuration Management
CP	Control Plane
CU/DU	Central Unit/Distributed Unit
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DNSSec	Domain Name System Security extensions
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECC	Elliptic-Curve Cryptography

ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDLP	Elliptic Curve Discrete-Log Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECP	Extended Cutting Plane
eMBB	enhanced Mobile Broadband
ESP	Encapsulating Security Payload
FM	Fault Management
GKDF	Generic Key Derivation Function
gNB	NR Node B
GUTI	Globally Unique Temporary Identifier
HMAC	Hash-based Message Authentication Code
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
ICV	Integrity Check Value
IPsec	Internet Protocol Security
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IMT-2020	International Mobile Telecommunications-2020
IP	Internet Protocol
IPX	IP exchange
JOSE	Javascript Object Signing And Encryption
JSON	JavaScript Object Notation
JWE	JSON Web Encryption
JWS	JSON Web Signature
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
LTE	Long-Term Evolution
LWE	Learning With Errors
MAC	Message Authentication Code
mIoT	massive Internet of Things
mMTC	massive Machine-Type Communication
MNO	Mobile Network Operator
MODP	Modular exponential
MPLS	Multiprotocol Label Switching
N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum

NDS	Network Domain Security
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NG-RAN	Next Generation-Radio Access Network
NP	Non-deterministic Polynomial time
NRF	NF Repository Function
NSSF	Network Slice Selection Function
NTRU	*N*th degree Truncated Polynomial Ring
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PKI	Public-Key Infrastructure
PKE	Public-Key Encryption
PM	Performance Management
PRF	Pseudo-Random Function
PSK	Pre-Shared Key
RLC	Radio Link Control
R-LWE	Ring Learning With Errors
RRC	Radio Resource Control
RSA	Rivest, Shamir and Adelman
PLMN	Public Land Mobile Network
PQC	Post-Quantum Cryptography
SBA	Service-Based Architecture
SDAP	Service Data Adaptation Protocol
SDN	Software-Defined Network
SEAF	Security Anchor Function
SEPP	Security Edge Protection Proxy
SHA	Secure Hash Algorithm
SIDF	Subscription Identifier De-concealing Function
SIDH	Supersingular-Isogeny Diffie–Hellman
SIKE	Supersingular Isogeny Key Encapsulation
SMF	Session Management Function
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SVP	Shortest Vector Problem

TLS	Transport Layer Security
TM	Trace Management
UDM	Unified Data Management
UDR	User Data Repository
UE	User Equipment
UOV	Unbalanced Oil and Vinegar
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communication
USIM	Universal Subscriber Identity Module
VNF	Virtual Network Function
WLAN	Wireless Local Area Network
XMSS	extended Merkle Signature Scheme

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 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 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 **"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

The IMT-2020 mobile communication technology is positioned to meet the business needs of the year 2020 and beyond. Security architecture is key to enabling normal operation of an IMT-2020 network. In fourth generation/long-term evolution (4G/LTE), only symmetric algorithms are utilized to protect signalling and user data. In addition to these, IMT-2020 systems introduce asymmetric algorithms to protect not only subscriber identifiers, but also communication between mobile network operators (MNOs).

Recently (as of September 2020), IBM has announced the 50 qubit quantum computer [b-QC1]. This breakthrough has dispelled the original anticipation that large-scale quantum computers would be on the market in 20 years. The new report [b-QC2] now estimates that 10 years is a realistic forecast for their availability.

The security of public-key cryptographic algorithms depends on the difficulty of computational problems, such as integer factorization or the discrete logarithm problem over various groups. It is showed that quantum computers can efficiently solve each of these problems [b-Shor 1997], thereby making all public-key cryptosystems based on such assumptions impotent. Thus, a sufficiently

powerful quantum computer will put at risk many forms of modern cryptosystems, such as key exchange, encryption and digital authentication.

Quantum computers will affect the security strength of symmetric and asymmetric algorithms to a different degree. Symmetric cryptographic strength will be halved, e.g., an advanced encryption standard (AES) with 128 bit keys giving 128 bit strength will be reduced to that of 64 bits, whereas many commonly used asymmetric algorithms, such as Rivest, Shamir and Adelman (RSA), digital signature algorithm (DSA) and elliptic-curve cryptography (ECC), will offer no security.

The IMT-2020 system aims to provide a wide range of services with different performance requirements. The services provided in IMT-2020 networks can be classified into enhanced mobile broadband (eMBB), massive Internet of things (mIoT) and ultra-reliable and low-latency communications (URLLCs).

The IMT-2020 system introduces a number of innovative technologies, such as network slicing, network function virtualization (NFV), the software-defined network (SDN) and service-based architecture (SBA). These technologies make the IMT-2020 system a flexible platform enabling new business cases and integrating vertical industries. On the other side, they make the security architecture of the IMT-2020 system much more complicated than previous mobile network generations.

There is a high desire to study how to protect communications in IMT-2020 systems by using quantum-safe algorithms. This is because it is likely that commercial quantum computers will become available within the lifecycle of IMT-2020 systems. Currently, the key length of symmetric algorithms specified for IMT-2020 systems is 128 bits. The 3rd Generation Partnership Project (3GPP) has just initiated a study item to research how to apply 256 bit key length symmetric algorithms to IMT-2020 systems [b-3GPP TR 33.841]. However, to date there has been no organization to study how to apply quantum-safe asymmetric algorithms to IMT-2020 systems. Some adaptation has to be made when quantum-safe cryptographic algorithms are used in IMT-2020 systems, since they have a longer key length than those used in classical cryptography. Moreover, there is a need to study how keys of different size coexist in IMT-2020 systems, since it is impossible to replace all classical algorithms with those that are quantum-safe overnight. A transition to quantum-safe cryptography in IMT-2020 systems should be considered early, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive.

In this Recommendation, the threats to IMT-2020 systems due to quantum computers are assessed. Quantum-safe algorithms are briefly reviewed, but their details are not specified in this Recommendation. The security guidelines recommend, at a high level, the adaptation of quantum-safe algorithms to IMT-2020 systems. This Recommendation provides the comprehensive guidelines to the application of quantum-safe symmetric and asymmetric algorithms to IMT-2020 systems, as well as the alignment of security levels between quantum-safe symmetric and asymmetric algorithms.

7 Introduction to security components of IMT-2020 systems

This clause provides background information for the security components of IMT-2020 systems, which have been specified in ITU-T, 3GPP, ETSI, IETF, etc.

A communication system should be able to provide some of the following security services to ensure the security of the system or data transmission [ITU-T X.800]: access control (authorization); authentication; privacy; confidentiality; data integrity; non-repudiation; and availability.

Security services could be achieved by using cryptographic or non-cryptographic mechanisms. This Recommendation focuses on the former, since it studies the application of quantum cryptographic algorithms to IMT-2020 systems.

In accordance with the architecture of IMT-2020 systems introduced in Appendix I, the security architecture of IMT-2020 systems can be described in three layers: infrastructure layer, network layer, and management plane.

7.1 Security of the infrastructure layer

The infrastructure layer is the common base to support the upper layer in IMT-2020 systems, which encompasses SDN and network function virtualization infrastructure (NFVI) layer.

7.1.1 Security of SDN

SDN technology is used for data delivery in IMT-2020 due to its dynamic and flexible management of traffic flows. The security architecture of SDN is specified in [ITU-T X.1038], which is simply illustrated in Figure 1.

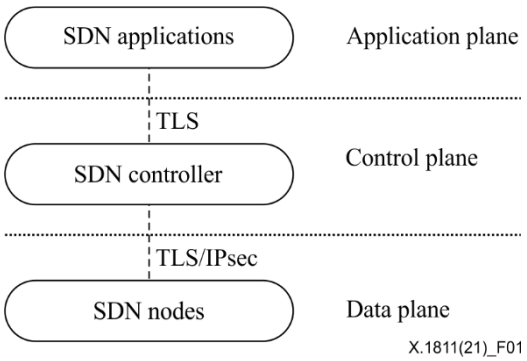

Figure 1 – Security architecture of SDN

[ITU-T X.1038] specifies the following recommendations relating to cryptographic algorithms and protocols.

The deployment of the transport layer security (TLS) [b-IETF RFC 5246] protocol is recommended to be put in place in the interface between the SDN application and the SDN controller. Based on TLS, the SDN application and the SDN controller authenticate each other and agree upon the session key; in addition, data confidentiality and data integrity over the application control interface are ensured.

The deployment of the TLS [b-IETF RFC 5246] protocol or Internet protocol security (IPSec) protocols ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]) is recommended to be put in place in the interface between the SDN controller and the SDN node. Based on TLS or IPsec, the SDN node and the SDN controller authenticate each other and agree upon the session key; in addition, data confidentiality and data integrity over the control note interface are ensured.

Authentication mechanisms could be based on either a pre-shared key (PSK) [b-IETF RFC 4279] [b-IETF RFC 4306] or a certificate [b-IETF RFC 4306] and [b-IETF RFC 5246]. Either RSA [b-ONF TR-511] or digital signature algorithms can be applied in certificate-based authentication. The Diffie-Hellman (DH) or elliptic curve Diffie-Hellman (ECDH) key exchange protocol can be implemented in the context of TLS or IPsec to agree upon the shared key between the two entities.

Cryptographic algorithms used for data encryption could be AES [b-NIST FIPS 197], Blowfish [b-Schneier] or 3DES [b-NIST SP 800-67]. Cryptographic algorithms used for data integrity mechanisms could be message authentication code (MAC) [b-IETF RFC 2104], hash-based message authentication code (HMAC) [b-IETF RFC 2104] or digital signature [b-NIST FIPS 186-4].

7.1.2 Security of the NFVI layer

The NFVI layer supports the running of virtual network functions (VNFs), whose structure is depicted in Figure 2.

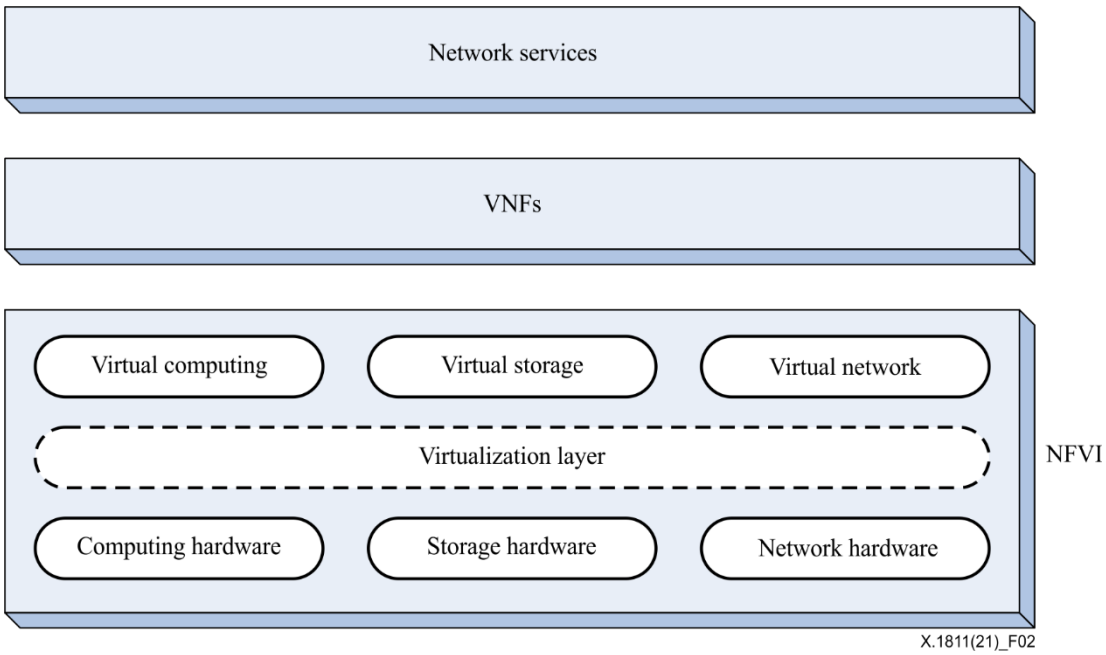

Figure 2 – NFVI structure (adapted from Figure 1 of [b-ETSI GS NFV 002])

According to [b-ETSI GS NFV-SEC 012], the NFVI shall support the following security functions to ensure the security of VNFs running on top of it: secure logging; operating system-level access and confinement control; physical controls and alarms; authentication controls; access controls; communications security; attestation; hardware-mediated execution enclaves; hardware-based root of trust; self-encrypting storage; direct access to memory; hardware security modules; and software integrity protection and verification. For this, the NFVI shall implement the following cryptographic algorithms [b-ETSI GS NFV-SEC 012]:

1) hashing algorithms: SHA-256, SHA-384, AES128-GMAC, HMAC-SHA128, HMAC-SHA256, HMAC-SHA384;
2) encryption algorithms: AES-CBC-128, AES-GCM-128 (16 octet integrity check value (ICV)), AES-CBC-256, AES-GCM-256 (16 octet ICV);
3) signature: RSA 2048, RSA 3072, RSA 4096, ECDSA-256 (secp256r1), ECDSA-384 (secp384r1);
4) public-key infrastructure (PKI): RSA 2048, RSA 3072, RSA 4096, id-ecPublicKey (secp256r1);
5) key exchange: DH group 14 (2 048 bit modular exponential (MODP)), DH group 19 (256 bit random extended cutting plane (ECP) group), DH group 20 (384 bit random ECP group), elliptic curve Diffie-Hellman ephemeral (ECDHE) secp256r1 (P-256), Diffie-Hellman ephemeral (DHE) groups of at least 2048 bits;
6) Pseudo-random function (PRF): PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384.

7.2 Security of the network layer

7.2.1 Security of the access network

The security of the access network [b-3GPP TS 33.501] is intended to ensure that authenticated user equipment (UE) is able to gain access to an IMT-2020 network, the communication between UE and the IMT-2020 network could be protected in a selectable fashion according to MNO security policy.

The security architecture for the IMT-2020 access network is illustrated in Figure 3, which can be specified as follows. The UE tries to gain access to the network with a temporarily assigned identity or concealed permanent identity before invoking the authentication and key agreement (AKA) protocol. The UE and the network mutually authenticate and agree upon a session key by running the AKA protocol. The UE and the network derive a set of keys based on the session key. Based on these keys, the integrity and reply protection of non-access stratum (NAS) signalling messages exchanged between the UE and access and mobility management function (AMF) are mandatory, while their confidentiality protection is optional; the integrity and reply protection of access stratum (AS) signalling messages exchanged between the UE and NR Node B (gNB) are mandatory, while their confidentiality protection is optional. Confidentiality and integrity protection of the user data in the user plane (UP) between the UE and the gNB are optional . The communication between UE and non-3GPP interworking function (N3IWF) is protected by using an IPsec tunnel in the case of non-3GPP access. As gNB-DU and gNB-CU could be deployed at different locations, the F1 interface between them is protected by applying network domain security/Internet protocol (NDS/IP). Similarly, an E1 interface between a gNB-CU-CP and gNB-CU-UP is secured on the basis of an NDS/IP. The backhaul network that connects a gNB to a core network is protected by using an NDS/IP, unless there is a physical protection in the backhaul network. As a user plane function (UPF) could be deployed at the network edge, the communication between the UPF and session management function (SMF) is also secured by using NDS/IP. Related to the security architecture of the access network, the following security services or functions are briefly surveyed:

– subscriber privacy;
– authentication;
– key hierarchy;
– security of NAS signalling, AS signalling, and user data;
– NDS/IP;
– security of non-3GPP access.

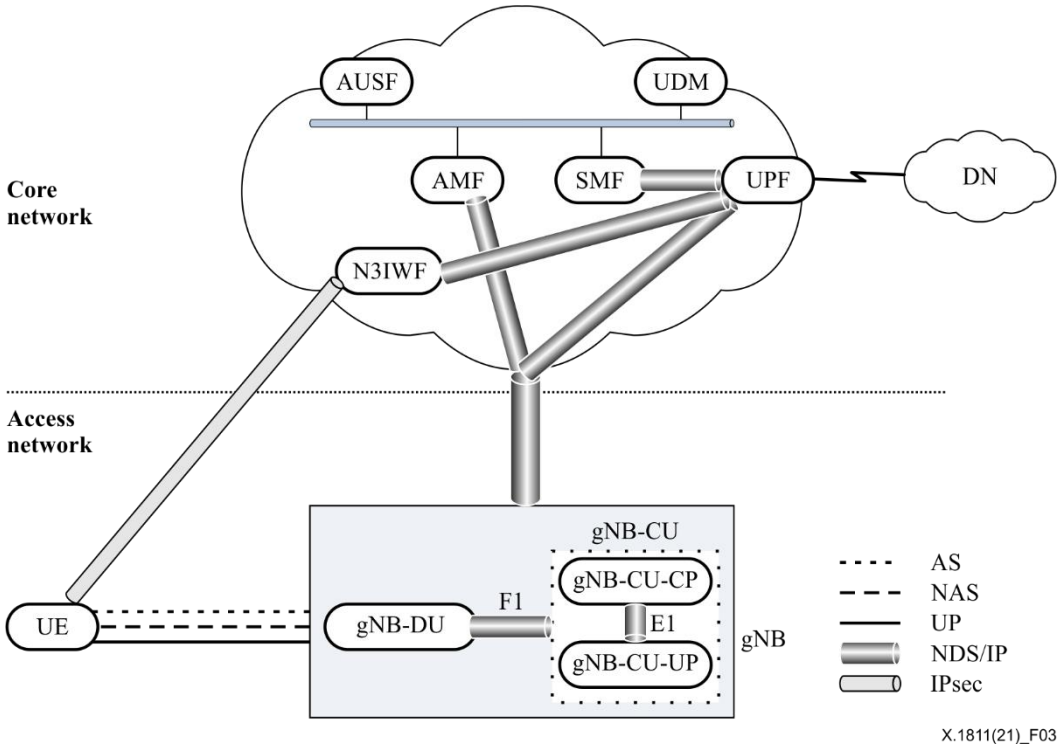

Figure 3 – Security architecture of access network

7.2.1.1 Subscriber privacy

A UE is assigned a globally unique subscription permanent identifier (SUPI) in the IMT-2020 system, which will be provisioned in the universal subscriber identity module (USIM) and unified data management/user data repository (UDM/UDR). A SUPI is never transmitted in the clear over the air interface when an IMT-2020 USIM is deployed. For initial access, the UE generates the subscription concealed identifier (SUCI), and transmits it to the UDM/ARPF (unified data management/authentication credential repository and processing function), as shown in Figure 4. Upon receipt of a SUCI, the subscription identifier de-concealing function (SIDF) located at the ARPF/UDM performs de-concealment of the SUPI from the SUCI. Based on the SUPI, the UDM/ARPF chooses the authentication method according to the subscription data.

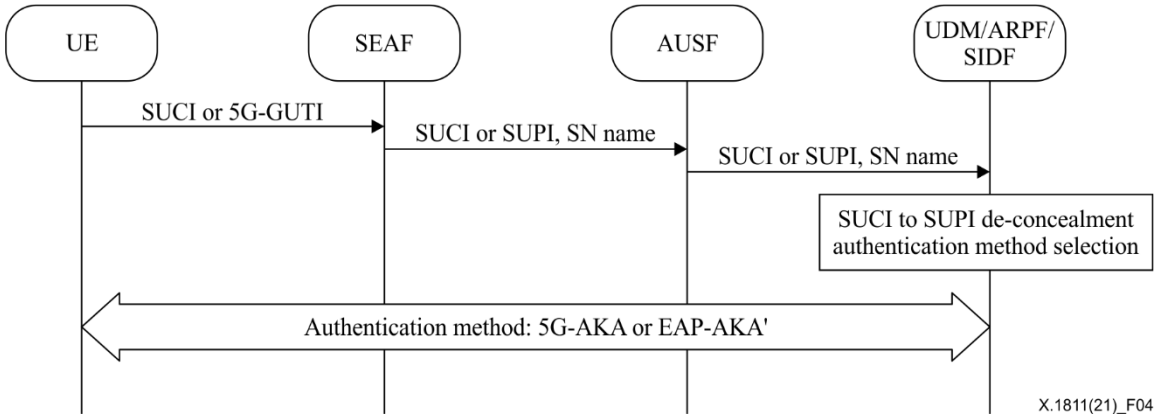

Figure 4 – Initial authentication procedure and selection of the authentication method (adapted from Figure 6.1.2-1 of [b-3GPP TS 33.501])

A SUCI is composed of a clear part and an encrypted part. The former contains the mobile country code and mobile network code, as information pertaining to the home network for routing the SUCI to the targeted UDM/ARPF. The latter contains sensitive subscription information, namely the mobile identification number, which is encrypted by using the elliptic curve integrated encryption scheme (ECIES). The public key of the home network is securely provisioned in the USIM and SIDF, respectively. The principle of ECIES is that the UE and the network apply their own private key and partner public key to agree on shared keys by using the ECDH mechanism. Based on the shared keys, data confidentiality and integrity protection are performed by using symmetric encryption algorithms and MAC algorithms, respectively. According to the profiles specified in [b-3GPP TS 33.501], ECDH mechanisms (X25519, elliptic curve cofactor DH primitive) are used to generate the shared keys, AES-128 in counter mode and HMAC-SHA-256 are used for data confidentiality and data integrity, respectively.

After the initiation of the authentication procedure, the UE is securely assigned an IMT-2020 globally unique temporary identifier (5G-GUTI) to conceal the SUPI in the subsequent authentication procedure.

7.2.1.2 Authentication

The IMT-2020 system applies two kinds of AKA protocol for mutual authentication between UE and the network as well as the generation of session key K_{SEAF}, which are 5G-AKA and extensible authentication protocol-authentication and key agreement (EAP-AKA'). The latter can be used for 3GPP and non-3GPP access. Compared to those for 4G, IMT-2020 authentication protocols provide increased home control to mitigate possible fraud charging from the roaming network. In the case of EAP-AKA', the UE identity verification at the network side is executed at the authentication server function (AUSF) of the home network. In the case of 5G-AKA, although the UE identity verification at the network side is performed at the security anchor function (SEAF) of the roaming network, the

AUSF of the home network will verify the authentication confirmation during each authentication procedure.

A set of key generation algorithms (*f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 and *f*5*) is used in the authentication procedure to generate the authentication vector (AV) and authentication response. There are two kinds of algorithm sets available for this. One is called the MILENAGE algorithm set [b-ETSI 135 205], where AES-128 is recommended as the base. The other is called the TUAK algorithm set [b-ETSI 135 231], where the Keccak sponge function [b-Bertoni] is used as the base, whose input key size can be either 128 bits or 256 bits. Note that in practice the MILENAGE algorithm set is more widely deployed than that of TUAK.

7.2.1.3 Key hierarchy

Based on the root key K, the UE and the network perform mutual authentication and generate the session key K_{SEAF}, which is the anchor for the keys (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) used for securing the communication between the UE and the network, as depicted in Figure 5.

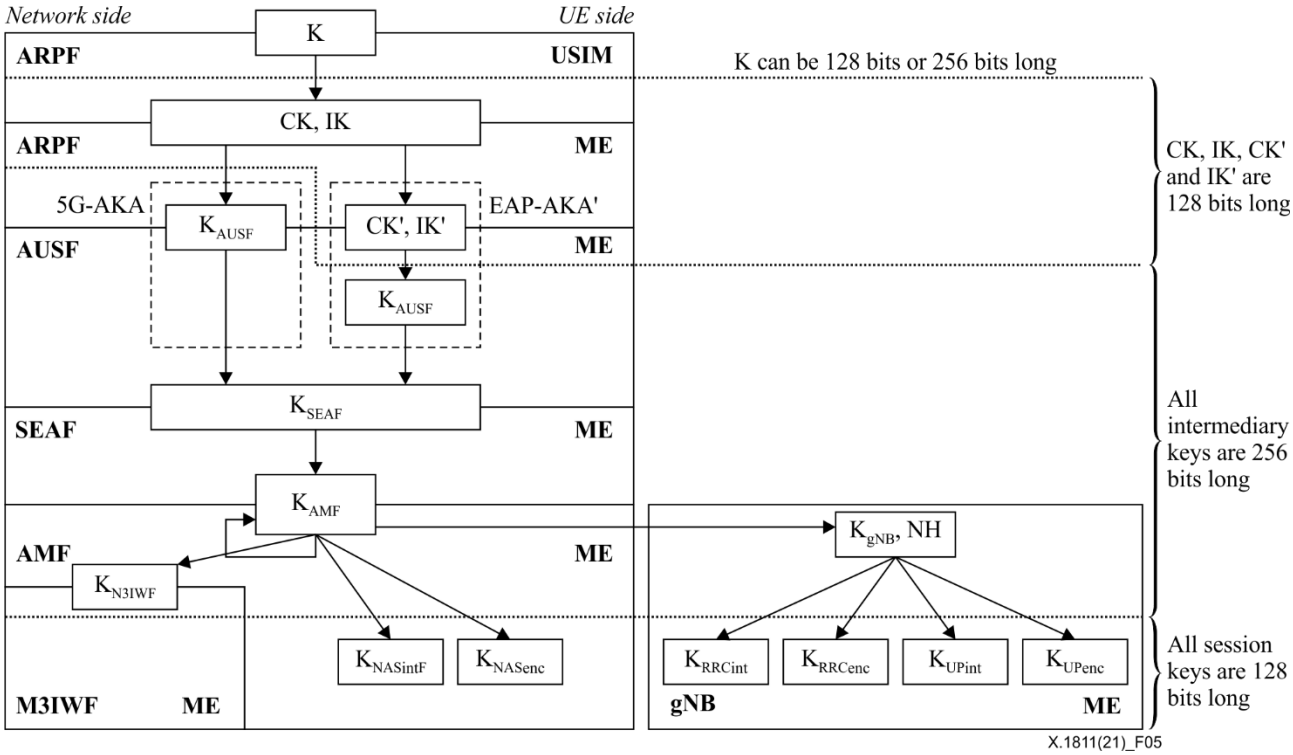

Figure 5 – Key hierarchy (adapted from Figure 6.2.1-1 of [b-3GPP TS 33.501])

The length of the root key K can be either 128 bits or 256 bits. It is worth noting that root key K in the legacy USIM is just 128 bits long, which means that only 128 bit long root keys are provisioned in the UDM for the corresponding USIM.

CK, IK, CK' and IK' are the keys related to the authentication procedure, whose length is 128 bits. The generation of CK and IK relies on either the MILENAGE or TUAK algorithm set, while the generic key derivation function (GKDF) defined in [b-3GPP TS 33.220] is used to produce CK' and IK'.

All intermediary keys are 256 bits long, whose generation relies on the GKDF except the key K_{AUSF} in the protocol EAP-AKA'. The HMAC-based extract-and-expand key derivation function (HKDF) specified in [b-IETF RFC 5869] is used to generate K_{AUSF} in the protocol EAP-AKA'.

The keys (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) used for securing the communication between UE and the network are 128 bits long, which are truncated from the 256 bit output of the GKDF.

7.2.1.4 Security of NAS signalling, AS signalling, and user data

To ensure the confidentiality of NAS signalling, AS signalling, and user data, the IMT-2020 system shall support 128-NEA1 (128 bit SNOW 3G-based algorithm) and 128-NEA2 (128 bit AES-based algorithm). In addition, a 128-NEA3 (128 bit ZUC-based algorithm) may be supported in the IMT-2020 system.

To ensure the integrity of NAS signalling, AS signalling, and user data, the IMT-2020 system shall support 128-NIA1 (128 bit SNOW 3G-based algorithm) and 128-NIA2 (128 bit AES-based algorithm). In addition, 128-NIA3 (128 bit ZUC-based algorithm) may be supported in the IMT-2020 system.

7.2.1.5 NDS/IP

The interfaces between the access network and core network (i.e., N2 interface between gNB and AMF, N2 interface between N3IWF and AMF, N3 interface between gNB and UPF, N3 interface between N3IWF and UPF), the interfaces between gNB-DU and gNB-CU (F1 interface), and interfaces between gNB-CU-CP and gNB-CU-UP (E1 interface) are protected by applying NDS/IP ([b-3GPP TS 33.210], [b-3GPP TS 33.310]), which specifies the security profile used in the 3GPP systems for IPsec, Internet key exchange version 2 (IKEv2), TLS and datagram transport layer security (DTLS) [b-IETF RFC 6083].

To protect the integrity and confidentiality of data transmitted over the N2 interface, E1 interface and F1 interface, as well as to prevent replay attacks, IPsec encapsulating security payload (ESP) and IKEv2 certificate-based authentication are recommended for implementation. In addition, DTLS shall be supported.

In order to provide integrity, confidentiality and reply-protection to traffic over the N3 interface, IPsec ESP and IKEv2 certificate-based authentication is recommended for implementation.

As ESP encryption algorithms, advanced encryption standard-cipher blocker chaining (AES-CBC) and advanced encryption standard-Galois counter mode (AES-GCM) with a 16 octet ICV shall be supported, in addition to AES-256. As ESP authentication algorithms, HMAC-SHA1-96 and the advanced encryption standard-Galois message authentication code (AES-GMAC) with AES-128 shall be supported.

Relating to IKEv2, the following algorithms shall be supported:

– confidentiality: ENCR_AES_CBC with a 128 bit key length, AES-GCM with a 16 octet ICV with 128 bit key length;
– pseudo-random function: PRF_HMAC_SHA1, PRF_HMAC_SHA2_256;
– integrity: AUTH_HMAC_SHA256_128;
– DH group 14 (2 048 bit MODP),19 (256 bit random ECP group);

Relating to IKEv2, for a high level of security, the following algorithms should be supported:

– confidentiality: AES-GCM with a 16 octet ICV with a 256 bit key length;
– pseudo-random function: PRF_HMAC_SHA2_384;
– DH group 20 (384 bit random ECP group).

DTLS 1.2 shares the same cipher suites as the TLS 1.2, as DTLS 1.2, as specified in [b-IETF RFC 6347], is based on TLS 1.2 The allowed and mandatory cipher suites given in TLS 1.2 [b-IETF RFC 5246] shall be followed. In addition, the following cipher suites are mandatory to support and recommended for use:

– TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in [b-IETF RFC 5289];

– TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in [b-IETF RFC 5288].

For a high level of security, support of the following cipher suites is recommended:

– TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in [b-IETF RFC 5289];

– TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in [b-IETF RFC 5289].

Relating to the DH groups, for ECDHE, the curve secp256r1 (P-256) as defined in [b-IETF RFC 4492] shall be supported; secp384r1 (P-384) as defined in [b-IETF RFC 4492] should be supported. For DHE, DH groups of at least 4 096 bits should be supported; DH groups smaller than 2 048 bits shall not be supported.

PSK-based authentication is allowed for use in the IKEv2, TLS handshake in the context of NDS/IP.

7.2.1.6 Security of non-3GPP access

Security of non-3GPP access is achieved by establishing an IPsec tunnel between UE and N3IWF. IKEv2 [b-IETF RFC 7296] is used to perform mutual authentication between UE and N3IWF on the basis of the key K_{N3IWF}, in order to set up one or more IPsec ESP [b-IETF RFC 4303] security associations for IPsec tunnels.

The communication security between N3IWF and AMF (N2 interface), as well as between N3IWF and UPF (N3 interface) is ensured by using NDS/IP.

7.2.2 Security of the core network

It is anticipated that IMT-2020 core network will be constructed on the basis of an NFV framework [b-ETSI GS NFV 002], where network functions (NFs) are decoupled from the dedicated hardware for rapid service deployment and improved operational efficiencies. As shown in Figure 6, the NFV framework can be divided into three layers denoted: NFVI; VNFs; and network services. VNFs run on top of the common NFVI layer to provide the desired network services. The security of the core network is essentially that of the VNF layer.

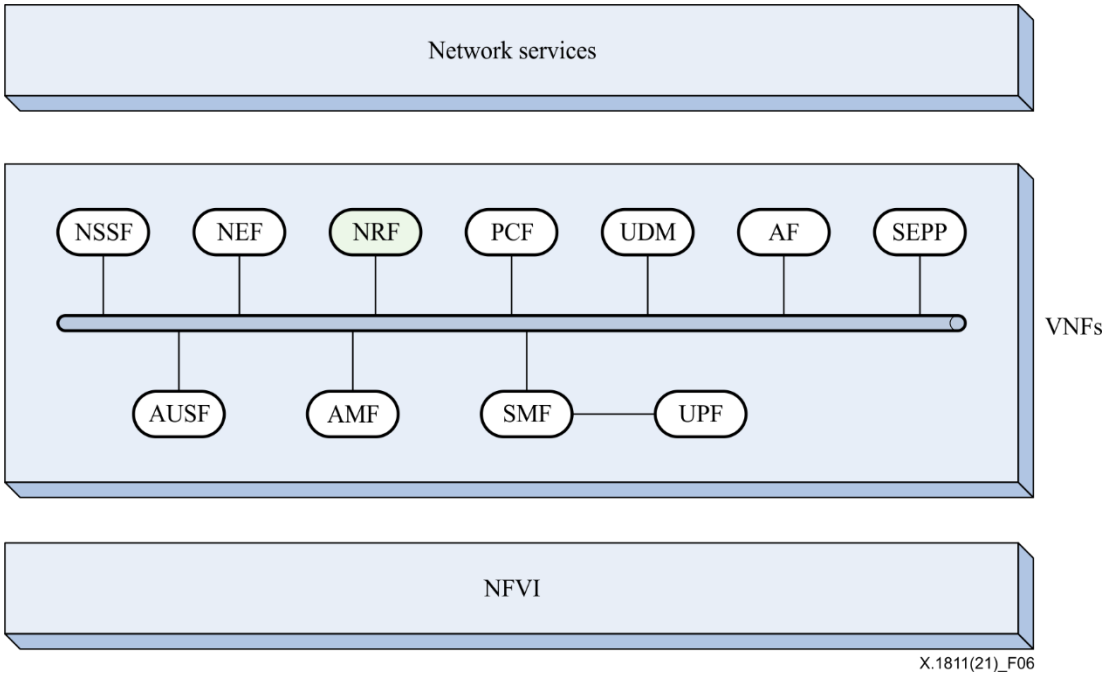

Figure 6 – Framework of NFV-based IMT-2020 core network (adapted from Figure 1 of [b-ETSI GS NFV 002]

VNFs are organized in an SBA, where the NF repository function (NRF) plays a key role in the system. The NRF decides whether an NF is authorized to perform discovery and registration, and issues the access token to the NF. The security of VNF layers can be considered within a public land mobile network (PLMN) and inter-PLMNs, respectively.

7.2.2.1 Within a PLMN

1) Authentication

The NRF and NF shall be mutually authenticated during the process of discovery, registration and access token request. This can be achieved by using either the NDS/IP or physical security. Authentication between NFs can be performed in the same manner.

2) Authorization

– **Static authorization**

After a service consumer NF and a service producer NF authenticate each other, the service producer NF shall check authorization of the service consumer NF based on local policy before granting access to the service application programming interface (API).

– **OAuth 2.0 based authorization**

The access control of network services provided by NFs can be implemented by using an OAuth 2.0 framework, specified in [b-IETF RFC 6749]. Access tokens shall be JavaScript object notation (JSON) web tokens as described in [b-IETF RFC 7519], secured with digital signatures or MAC digital signatures based on a JSON web signature (JWS) as described in [b-IETF RFC 7515]. The NRF acts as the OAuth 2.0 authorization server. The NF service consumer and the NF service producer correspond to the OAuth 2.0 client and the OAuth 2.0 resource server, respectively. The communication between NFs and the NRF is protected by using TLS, since credentials are transmitted among them.

7.2.2.2 Inter-PLMNs

Security of inter-PLMNs is enabled by security edge protection proxies (SEPPs) of both networks over an N32 interface, as shown in Figure 7.

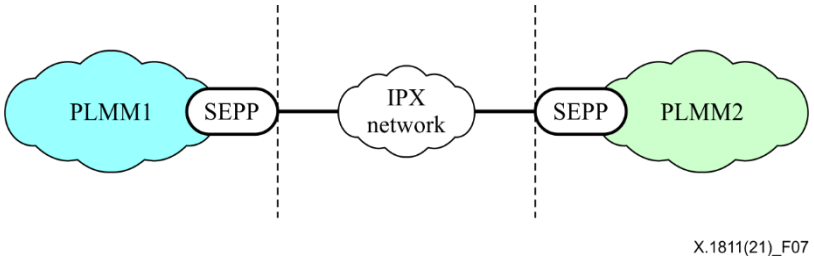

Figure 7 – Security of inter-PLMNs

The N32 interface consists of an N32-c connection and an N32-f connection. The former is responsible for management of the N32 interface, including a mutual AKA between the two SEPPs by using TLS. The latter vouches for sending of messages protected by Javascript object signing and encryption (JOSE) between the SEPPs.

The SEPPs use JSON web encryption (JWE, specified in [b-IETF RFC 7516]) for protecting messages on the N32 interface, where agreed keys between two SEPPs in N32-c connection are applied. The IP exchange (IPX) providers apply JWSs, specified in [b-IETF RFC 7515], to sign the modifications needed for their mediation services.

All entities and functions that support JWE shall use the following algorithms [b-3GPP-TS 33.210]: "enc" parameter A128GCM (AES-GCM with a 128 bit key) shall be supported. "enc" parameter A256GCM (AES-GCM using a 256 bit key) should be supported. "alg" parameter "dir" (direct use of a shared symmetric key as the content encryption key (CEK)) shall be supported.

All entities and functions that support JWS shall use the following algorithms [b-3GPP-TS 33.210]: "alg" parameter ES256 (elliptic curve digital signature algorithm (ECDSA) using P-256 and secure hash algorithm-256 (SHA-256)) shall be supported.

7.3 Security of the management plane

The management plane consists of a manager set (NFV orchestrator, VNF manager, virtualized infrastructure manager, SDN controller, RAN manager). This manager set takes charge of the management of configuration, performance and faults of the corresponding objectives via interfaces. Any modification, deletion, insertion or replay shall be prevented during the data transfer between the manager and managed objective [b-ETSI GS NFV-SEC 014]. For this, TLS is applied to these interfaces by default in the industry, as shown in Figure 8.

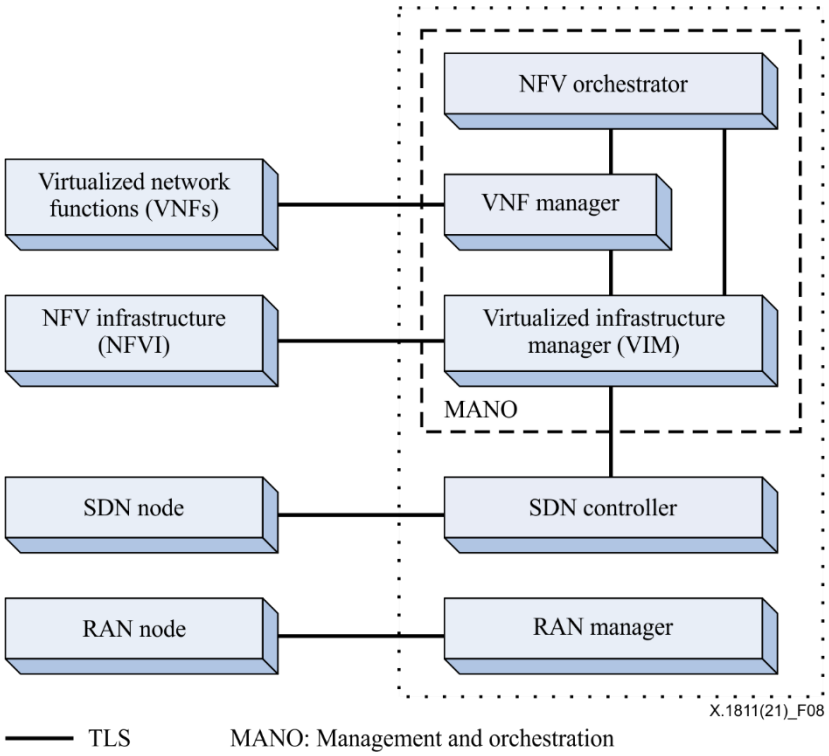

Figure 8– Security of the management plane

7.4 Summary of the cryptographic algorithms used in IMT-2020 system

Based on the introduction to the security architecture of IMT-2020 system in clauses 7.1 to 7.3, the cryptographic algorithms used in IMT-2020 system can be summarized in Table 1.

Table 1 – Cryptographic algorithms used in the IMT-2020 system

Type	Name	Function	Application scenario
Symmetric cryptographic algorithms	128-NEA1	Encryption	Confidentiality protection between UE and AMF, as well as between UE and gNB
	128-NEA2		
	128-NEA3		

Table 1 – Cryptographic algorithms used in the IMT-2020 system

Type	Name	Function	Application scenario
	128-NIA1	MAC	Integrity protection between UE and AMF, as well as between UE and gNB
	128-NIA2		
	128-NIA3		
	AES-128	Encryption	IPsec, TLS, DTLS, JWE, ECIES, NFVI
	AES-256	Encryption	IPsec, TLS, DTLS, JWE, NFVI
	Blowfish	Encryption	SDN
	3DES	Encryption	SDN
	SHA-256	Hashing	IPsec, TLS, DTLS, JWS, NFVI
	SHA-384	Hashing	IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-256	Key derivation/ MAC /Pseudo Random Function	Key hierarchy IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-384	Key derivation/ MAC /Pseudo Random Function	IPsec, TLS, DTLS, JWS, NFVI
Asymmetric cryptographic algorithms	RSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	ECDSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	DH	Key agreement	IPsec, TLS, DTLS, NFVI
	ECDH	Key agreement	IPsec, TLS, DTLS, NFVI
NOTE 1 – SHA-1 is not listed due to its weak security strength. NOTE 2 – The key size of currently used asymmetric cryptographic algorithms is not marked since these algorithms can be broken regardless of the key size if the large-scale quantum computer is available. NOTE 3 – The version of TLS is not less than 1.2 for security reasons.			

8 Security assessment of IMT-2020 systems under quantum computing

A quantum computer is a device that exploits quantum mechanical phenomena (superposition and entanglement) to perform calculations and manipulate data. The security foundation of the currently popular cryptographic algorithms is built on some intractable mathematical problems. Due to the intrinsic parallelism attribute of a quantum computer, some quantum algorithms can solve difficult mathematical problems more efficiently than classical ones. This poses serious and realistic security threats to contemporary cryptography. Appendix III lists the impact of quantum computing on common cryptographic algorithms. In clause 8.1, the threats to conventional cryptographic algorithms due to the availability of quantum computers are introduced. Then, the impacts on IMT-2020 systems raised by quantum computers are analysed.

8.1 Threats to conventional cryptographic algorithms

8.1.1 Asymmetric cryptographic algorithms

The Shor algorithm can solve the factoring large integer problem and discrete-log problem in a polynomial time [b-Shor 1999]. This undermines the security of current popular asymmetric algorithms. This means that RSA-based public-key cryptography, whose security relies on the factoring large integer problem, and DH key exchange protocol, whose security relies on the discrete-log problem, will offer no security. Like the DH algorithm, the security of the DSA algorithm

relies on the discrete logarithm. Therefore, the DSA algorithm is subject to quantum attacks. ECC, whose security relies on the elliptic curve discrete-log problem (ECDLP), has been widely deployed for their significant smaller key size compared to the RSA-based public-key system. However, it can be broken by using a variant of the Shor algorithm [b-Roetteler]. This implies that ECC, including the ECDSA and ECDH, are insecure if large-scale quantum computers are available. Table 2 lists the quantum resources required to break the asymmetric cryptographic algorithms that are currently widely used.

Table 2 – Quantum resource required to break the asymmetric cryptographic algorithms

Algorithms	Public-key size (bits)	Security level comparable to the symmetric algorithm (bits)	Logical qubits	Physical qubits (see Note 1)	Toffoli gates (see Note 1)	Time required to break algorithms (see Note 2)
RSA [b-Häner]	1 024	80	2 050	7.38×10^6	5.81×10^{11}	9.68 h
	2 048	112	4 098	1.48×10^7	5.2×10^{12}	3 days 14 h
	4 096	128	8 194	2.95×10^7	5.59×10^{13}	31days 21 h
ECC based [Roetteler]	256	128	2 330	8.39×10^6	1.26×10^{11}	2.1 h
	384	192	3 484	1.25×10^7	4.52×10^{11}	7.5 h
	521	256	4 719	1.69×10^7	1.14×10^{12}	19 h
NOTE 1 – Quantum computers require the extra physical quantum bits for error correction. The estimated number of physical qubits per logical qubit varies from 10 to 10 000. Here we assume one logical qubit per 3 600 physical qubits, see [b-Fowler]. NOTE 2 – We assume that operation time of a Toffoli gate is 60 ns, see [b-Banchi].						

8.1.2 Symmetric cryptographic algorithms

The Grover algorithm provides a quadratic speed-up to search in an unstructured data set over classic algorithms [b-Grover]. This can be exploited to search the key in the key space of a symmetric key algorithm. For a symmetric key algorithm with a key n bits long, the key can be found with $O(2^{n/2})$ quantum operations on the quantum machine instead of $O(2^n)$ classical operations on the conventional computer. The quantum resource required to search the key of a symmetric algorithm is so large that the implementation of the Grover algorithm to break the symmetric key algorithm on an actual physical quantum computer is questionable. For example, an exhaustive key search for an AES by using the Grover algorithm needs the following numbers of Toffoli and Clifford gates: 2^{86} for AES-128; 2^{118} for AES-192; and 2^{151} for AES-256, although the number of logical qubits required ranges from 3 000 to 7 000 [b-Grassl].

The Grover algorithm cuts the effective key size in half, i.e., it halves the security strength of a symmetric key algorithm. Thus to achieve quantum assistance, the key size of the symmetric key algorithm has to be doubled.

8.1.3 Hash algorithms

The Grover algorithm and its variant do not speed up the finding of hash collisions compared to the classical algorithm [b-Bernstein 2009]. The best approach would be to use a parallel version of Pollard's ρ method on a classical computer cluster [b-ETSI GR QSC 006]. This means that if currently used hash algorithms are secure, then they would be secure against quantum-computing attacks in the quantum era. SHA-256 that has been proved to be secure using classical computing has also been shown to be able to resist a quantum pre-image attack [b-Amy].

8.1.4 Key derivation functions

Key derivation functions (KDFs) are intended to generate the keys used for confidentiality and integrity protection, which are achieved by embedding the shared key into the hash functions. There are two kinds of KDFs deployed in the IMT-2020 system. One is the GKDF defined in [b-3GPP TS 33.220], the other is the HKDF specified in [b-IETF RFC 5869].

The base of the GKDF and HKDF is the keyed hash function HMAC-SHA-256. The security of HMAC depends on the cryptographic strength of the used hash function [b-IETF RFC 2104]. As a result, the KDFs used in IMT-2020 system themselves are not substantially affected by advances in quantum computing.

Note that the entropy of the output of the KDFs depends on the entropy of the input key used in the KDFs. For a 256 bit entropy output, a 256 bit entropy input key is needed when applying KDFs.

8.2 Prediction of the timeline for large-scale quantum computer

It is difficult to predict the exact timeline for the availability of large-scale quantum computers, because there is no consensus on this issue. [b-NISTIR 8105] estimates that a quantum computer costing 1 billion US dollars may break 2 048 bit RSA in 2030. The European Telecommunications Standards Institute (ETSI) has come to a similar conclusion that large-scale computers may be built in 2031 [b-ETSI GR QSC 004]. As a result, the security of IMT-2020 systems may be compromised as IMT-2020 systems will operate over a period lasting 10 to 20 years. On the other side, [b-NASEM] states that it is highly unlikely that a quantum computer breaking 2 048 bits RSA can be built in the next decade. This does not imply that quantum-safe cryptographic algorithms should not be studied and standardized now, since the time frame for transitioning to a new security algorithm is sufficiently long and uncertain [b-NASEM].

8.3 Impacts on IMT-2020 systems

As shown in clause 7, IPsec, TLS and DTLS have been deployed in many places in IMT-2020 networks. It is necessary first to give a general view to evaluate the threats to them raised by quantum computers. After that, impacts on the security of IMT-2020 systems will be assessed according to the structure introduced in clause 7.

8.3.1 Impacts on IPsec, TLS and DTLS

Although IPsec, TLS and DTLS run on different layers to protect message transmission (IPsec residing in the network layer, TLS and DTLS residing between the network and application layers), their design follows a similar principle. They are composed of two parts: one is the authentication and key establishment to generate session keys; the other is confidentiality and integrity protection of messages by using symmetric algorithms with the session keys.

There exist two methods to perform the authentication and key establishment, based on: (1) a pre-shared symmetric key; (2) a public key (usually a certificate is used).

For confidentiality and integrity protection, current cipher suits in IPsec, TLS and DTLS can support both 128 bit and 256 bit symmetric algorithms.

As a result, it can be assessed whether IPsec, TLS, and DTLS can withstand quantum-computing attacks by considering cases 1 to 4.

Case 1: Public-key based authentication and 128 bit or 256 bit symmetric algorithms

In this case, session keys can be recovered by the attackers since current specified asymmetric algorithms in Internet Engineering Task Force (IETF) standards can be broken by quantum computers due to the Shor algorithm. So, no matter how long the key size of symmetric algorithms is, the security of transmitted messages cannot be guaranteed.

Case 2: 128 bit PSK--based authentication and 128 bit symmetric algorithms

In this case, due to the Grover algorithm, the effective security key size is 64 bits if a large-scale quantum computer is available. Thus, these three protocols are not secure against quantum attack.

Case 3: 256 bit PSK--based authentication and 128 bit symmetric algorithms

In this case, although a 256 bit PSK is used for authentication and key establishment, only 128 bit symmetric algorithms are applied to message protection. Thus, the security strength of these three protocols is 64 bits.

Case 4: 256 bit PSK--based authentication and 256 bit symmetric algorithms

In this case, the effective security strength of these three protocols is 128 bits. So quantum attacks can be thwarted by using this cipher profile.

Only case 4 is secure against quantum attack for current cipher profiles. However, PSK--based authentication is just suitable for a small communication group as a PSK has to be manually configured in the corresponding devices. Public-key-based authentication is recommended to be applied when the communication group becomes large. For this, quantum-safe cryptographic asymmetric algorithms is recommended to be introduced in the above protocols (i.e., IPsec, TLS and DTLS) for authentication.

8.3.2 Impacts on the infrastructure layer

As shown in clause 7.1, TLS is used to protect the interface between applications and the SDN controller, as well as the interface between the SDN controller and SDN nodes. IPsec may be applied to the interface between the SDN controller and SDN nodes. Based on the analyses in clause 8.3.1, these two interfaces are subject to quantum attacks, i.e., attackers could eavesdrop, alter and inject messages transmitted over these two interfaces, unless the algorithms in case 4 are deployed in TLS and IPsec.

The NFVI layer is vulnerable to quantum attack since it relies on classical asymmetrical cryptographic algorithms to implement some security functions. This may lead to serious consequences, such as illegal access to the platformor planting of malicious software.

8.3.3 Impacts on the access network

8.3.3.1 Subscriber privacy

A SUPI is concealed by converting it into SUCI with the ECIES scheme as introduced in clause 7.2. The ECDH is used to agree the shared key between the UE and the network in the ECIES scheme. Attacks can recover the shared key due to the Shor algorithm if large-scale quantum computers are available. Consequently, the SUPI is disclosed to attackers by decrypting SUCI with the shared key.

8.3.3.2 Authentication

Both the 5G-AKA and EAP-AKA' protocol perform mutual authentication between the UE and the network based on the long-term key K, whose size may be 128 bits or 256 bits. As for the 256 bit key K, until now, there have been no attacks on the hash functions (i.e., the TUAK algorithm set) that are the base from which to derive various parameters used in the authentication protocol by using a classical computer. Thus, both authentication protocols are secure against quantum attacks, since there is no more efficient algorithm to break hash functions by using quantum computers than by using classical computers in the context of a 256 bit key K. As for a 128 bit K, whose effective security strength is 64 bits in the quantum era, attackers may recover the key K from the captured messages related to both authentication protocols, e.g., AVs, by performing 2^{64} quantum operations using the Grover algorithm.

8.3.3.3 Key hierarchy

Key hierarchy is used to derive 128 bit keys from the long-time (root) key K as shown in Figure 5, in order to protect communication between the UE and the network. Currently, the key K with 128 bits is widely deployed, while the key K with 256 bits is rarely applied. As for a 128 bits K, whose effective security strength is 64 bits in the quantum era, security strength of the derived keys is 64 bits. As a result, attacks could recover the keys from these captured messages encrypted with 128 bit keys.

8.3.3.4 NAS signalling, AS signalling, and user data

The confidentiality of NAS signalling, AS signalling and user data is protected by using symmetric algorithms with 128 bit long keys. Thus, these messages can be decrypted by attackers with quantum computers.

The integrity of NAS signalling, AS signalling and user data is protected by using MAC algorithms with a 128 bit key. The output of MAC algorithms is truncated into a 32 bits long tag that is used as a MAC tag. It is straightforward that an attacker can forge a message after 231 attempts if the MAC tag length is 32 bits. Whether the security of an IMT-2020 system is at risk if a 32 bit long MAC tag is truncated from the 64 bit native tag or 128 bit native tag needs further study.

8.3.3.5 NDS/IP

TLS, DTLS and IPsec are deployed to protect the N2 interface, N3 interface, E1 interface and F1 interface as introduced in clause 7.2.1. This poses the same impacts as the transport layer, i.e., attackers could eavesdrop, alter and inject messages transmitted over these interfaces, if the cipher suites in case 4 of clause 8.3.1 are not used.

8.3.3.6 Security of non-3GPP access

Non-3GPP access is secured by using IPsec. For the reasons introduced in clause 8.3.1, secure non-3GPP access cannot be guaranteed, unless the cipher suites in case 4 of clause 8.3.1 are used.

8.3.4 Impacts on the core network

8.3.4.1 Within a PLMN

1) Authentication

The authentication between NFs will not be affected if its operation relies on physical security. The authentication may be subject to the same threats as specified in clause 8.3.3 if it is achieved by using the NDS/IP.

2) Authorization

Static authorization will not be affected, as no cryptographic algorithm is applied.

For OAuth 2.0-based authorization, there are two scenarios to ensure the integrity of the access token. The adversary can fake an access token if its integrity is protected by using a signature. In contrast, an access token cannot be forged if a MAC with a 256 bit long key is applied to protect its integrity. The credentials used in authorization may be disclosed as they are transmitted over TLS between NFs, unless case 4 of clause 8.3.1 applies.

8.3.4.2 Inter-PLMNs

The attackers could eavesdrop, alter and inject messages transmitted over the N32 interface between PLMNs. The reason is that N32-c connection relies on certificate-based authentication in TLS to establish session keys, and attackers could acquire these keys by using quantum computers.

8.3.5 Impacts on the management plane

Any modification, deletion, insertion or replay during data transfer between the manager and managed objectives is possible, as TLS with certificate-based authentication is deployed in the management plane. This poses a serious threat to IMT-2020 systems, as it is possible for an attacker to gain access to the management system of the IMT-2020 network.

9 Quantum-safe cryptographic algorithms

Quantum computing introduces a completely new computing paradigm. This will affect the security of both symmetric-key algorithms (e.g., block ciphers) and public-key algorithms (such as RSA), although the seriousness of the impact will be different for each.

[b-Moses] shows thatquantum computing effectively halves the number of bits of key strength for any symmetric key algorithm and that quantum computers can run algorithms (e.g., that of [b-Grover]) and find a key of a symmetric cipher with an N bit key in $2^{N/2}$ operations. Thus, if quantum computing becomes a reality, symmetric key algorithms can be protected against this by simply doubling the key size. Of course, this will have an impact on the performance of the symmetric key algorithm.

As for asymmetric key algorithms, such as RSA, DSA, ECC and DH, the effect of quantum computing is thought to be quite serious. Quantum computers can run algorithms (e.g., that of [b-Shor 1997]) that break all popular public-key systems in trivial amounts of time. For instance, a quantum algorithm called Shor's algorithm can recover an RSA key in polynomial time [b-Moses].

Quantum-safe cryptographic algorithms should be selected by assessment criteria (see Appendix IV, for example, assessment criteria by NIST).

9.1 Quantum-safe symmetric key algorithms

It is widely believed that basic symmetric cryptosystems, such as block ciphers or hash functions are quantum-safe algorithms [b-CSA] as shown in Appendix III. [b-ITU-T X.1197] provides a list of examples of quantum-safe algorithms and key lengths. The advent of cryptographically-relevant quantum computers will notably require an increase in the symmetric key size, amounting to double the current 128-bit keys used in IMT-2020. [b-CSA] shows that the current recommended key size of 256 bits is considered safe, even against the Grover algorithm.

9.2 Quantum-safe asymmetric key algorithms

Although quantum computers can run algorithms that break current public-key systems (e.g., RSA and ECC) in trivial amounts of time as shown in Appendix III, there are many important classes of cryptographic system beyond RSA and ECC that are secure against an attack by a quantum computer and described in clauses 9.2.1 to 9.2.5. A list of the current standards for quantum-safe asymmetric algorithms is provided in [b-ITU-T X.1197].

NOTE – Quantum key distribution (QKD) is a method for implementing key agreement that is proven as robust against quantum computing.

9.2.1 Lattice-based algorithms

Lattice-based algorithms are based on some well-known difficult problems on the lattice to construct quantum-safe cryptographic primitives. One of these is the shortest vector problem (SVP),i.e., to find the shortest non-zero vector in a given lattice, which has been proven to be a non-deterministic polynomial time-hard (NP-hard) problem under randomized reductions [b-Ajtai].

[b-CSA] shows that lattice-based algorithms can provide digital signature, public or private key encryption and key agreement. Some lattice-based algorithms are listed in clause II.1.

9.2.2 Hash-based algorithms

Hash-based algorithms rely on the security of the underlying cryptographic hash function.

[b-CSA] shows that hash-based algorithms are used for digital signatures constructed using hash functions. Some hash-based algorithms are listed in clause II.2.

9.2.3 Code-based algorithms

Code-based algorithms rely on some error-correcting codes, where encoding schemes are difficult to decode efficiently, even for a quantum computer. For example, McEliece cryptosystem [b-McEliece] is based on the NP-hard problem of decoding a general linear code.

[b-CSA] shows that code-based algorithms can provide digital signature, public or private key encryption and key agreement. Some code-based algorithms are listed in clause II.3.

9.2.4 Multivariate algorithms

Multivariate algorithms are based on the difficulty of solving systems of nonlinear multivariate polynomial equations over finite fields. This problem is known to be NP-hard [b-Garey].

[b-CSA] shows that multivariate algorithms can provide digital signature and public or private key encryption. Some practical signature schemes based on multivariate algorithms are listed in clause II.4.

9.2.5 Supersingular isogeny-based algorithms

Supersingular isogeny-based algorithms are constructed on the basis of the difficulty of recovering an unknown isogeny between a pair of supersingular elliptic curves that are known to be isogenous.

They offer perfect forward security, and serve as a straightforward quantum-computing resistant replacement for the DH and ECDH methods. A typical example is the supersingular-isogeny Diffie-Hellman (SIDH) algorithm [b-Jao].

10 Guidelines for usage of quantum-safe cryptographic algorithms in IMT-2020 systems

General consideration is first given to the handling of the significant increase in message size when quantum-safe asymmetric algorithms are introduced into IMT-2020 systems. The usage of quantum-safe cryptographic algorithms in IPsec, TLS and DTLS is then taken into account, since they have been deployed at more than one place in IMT-2020 systems. Then guidelines to apply quantum-safe cryptographic algorithms to an IMT-2020 access network and IMT-2020 core network are specified, respectively.

10.1 Message size

The size of messages that contain a public key, ciphertext or signature will be significantly increased, since quantum-safe asymmetric algorithms usually have much larger size, relating to the public key, ciphertext or signature, than classical asymmetric algorithms. For example, the public-key size of quantum-safe asymmetric algorithms varies from 726 bytes to around 1 Mbyte as shown in clause II.5, while the public-key size of classical asymmetric algorithms typically varies from just 32 bytes to 256 bytes. The National Institute of Standards and Technology (NIST) plans to standardize more than one quantum-safe asymmetric algorithm. Thus, it is intuitive that quantum-safe asymmetric algorithms with smaller size of public key, ciphertext or signature needs to be chosen for use in IMT-2020 systems. Moreover, IMT-2020 system standards need to determine the appropriate message size to accommodate the public key, ciphertext or signature when quantum-safe asymmetric algorithms are deployed.

10.2 IPsec, TLS and DTLS

If a PSK is applied to authentication and key agreement, the size of the PSK is recommended to be 256 bits, and quantum-safe symmetric algorithms whose key length is 256 bits is recommended to be used for the confidentiality and integrity protection of messages transmitted over the network. If certificate-based authentication schemes are used, quantum-safe asymmetric algorithms is recommended to be integrated into the authentication protocols for a quantum-safe authentication and session key agreement, for the confidentiality and integrity protection of messages, quantum-safe symmetric algorithms with a 256 bit long key is recommended to be deployed. In this way, SDN, NDS/IP and the management plane are not vulnerable to quantum attacks.

IETF has not started work on how to add quantum-safe algorithms to the cipher suites in IPsec, TLS and DTLS, as NIST has not finalized the candidates for quantum-safe asymmetric algorithms. It is anticipated that NIST draft standards will be available in 2022 to 2024 [b-Moody]. Once IETF has specified the quantum-resistant cipher suites for IPsec, TLS and DTLS, considering the scarce wireless bandwidth and limited computation capabilities in devices, a cipher suite with smaller key size and high-speed encryption operation is recommended to be deployed in IMT-2020 systems.

10.3 Infrastructure layer

An SDN is recommended to apply the suggestions specified in clause 10.2 to the usage of IPsec and TLS.

The classical cryptographic algorithms deployed in the NFVI layer is recommended to be replaced with quantum-safe cryptographic algorithms, including those of the symmetric and asymmetric types.

10.4 IMT-2020 access network

10.4.1 Subscriber privacy

The ECIES scheme is recommended to apply DH-like quantum-safe asymmetric algorithms to generate the shared key, such as supersingular isogeny key encapsulation (SIKE) and NewHope, that are second round candidates in the NIST post-quantum cryptography (PQC) standardization procedure (see Appendix II). The SUCI is recommended to be concealed by the quantum-safe symmetric algorithm with a 256 bit shared key.

10.4.2 Authentication

Since the MILENAGE algorithm set supports only a 128 bit key input, while the TUAK algorithm set can support one of 256 bits, the TUAK algorithm set is recommended to be employed in the authentication procedure to generate the AV and authentication response instead of that of MILENAGE.

10.4.3 Key hierarchy

To generate the session key K_{SEAF} with 256 bit entropy, the key hierarchy has to make the following adaptations: (1) the key size of the root key K is recommended to be 256 bits; (2) 256 bit-long outputs of the GKDF is recommended to no longer be truncated.

In practice, the key length of the root key K is usually 128 bits, due to the use of legacy USIM cards in IMT-2020 systems that have that configuration; new USIM cards used for early IMT-2020 systems by many operators will still store only a 128 bit root key. A consequence is that the entropy of the session key K_{SEAF} derived from key K is only 128 bits, which is not quantum-safe.

To enhance the security for the current session key K_{SEAF} when the USIM card is equipped with a 128 bit long root key, the generation of the current session key K_{SEAF} is based on not only the first session key K_{SEAF}' determined by the long-term key K, but also at least one of the additional keys. The additional keys could be the initial session key $K_{SEAF\_INITIAL}$ generated the first time that the UE is connected to the network and/or the session key K_{SEAF_PRV} used in the previous session. Both the

first session key and the additional keys are symmetric keys, which means that the UE and the network share them. In this way, the entropy of the current session key K_{SAEF} will be at least 256 bits, since the entropy of the first session key K_{SEAF}' is 128 bits and the entropy of the additional keys (key $K_{SEAF\_INITIAL}$ and/or key K_{SEAF_PRV}) is at least 128 bits.

As a good practice, new SIM cards can optionally be used to achieve 256 bits entropy for the session key K_{SEAF}. Those can be either SIM, USIM or eSIMs or other non-standard SIM form factors and types with the corresponding adaptations so as to:

a) Store a 256-bit root key, to serve the same purpose as the root key K in old (U)SIMs.

b) Support hardware acceleration for the necessary KDF and symmetric cryptography core loop (e.g., AES) in the new SIM cards. This is particularly relevant for IoT and in countries where feature phones make an important part of the total number of cellular devices in use, yet could be made compatible with a quantum-safe – if not fast –, IMT-2020, through frequency reuse and protocol translation.

10.4.4 Security of NAS signalling, AS signalling and user data

As shown in clause 7, 128 bit symmetric key algorithms, such as AES-128, SNOW 3G, and ZUC-128 are the basis for confidentiality and integrity protection of NAS signalling, AS signalling, and user data in an IMT-2020 access network.

To resist quantum attacks, 256 bit symmetric key algorithms is recommended to be deployed in IMT-2020 systems. The longer MAC size provides greater assurance against attacks that guess the correct MAC for the message. [b-NIST SP 800-38B] recommends that at least a 64 bit long MAC is recommended to be used to defend against guessing attacks. The MAC length in an IMT-2020 access network is only 32 bits. There is a great impact on the IMT-2020 network and protocol if the MAC size is increased from 32 bits to 64 bits. Whether an IMT-2020 access network can still defend against guessing attacks when 256 bit quantum-safe symmetric algorithms are applied to generating a 32 bit long MAC needs further study.

10.4.5 Security of non-3GPP access

For the strategy to resist quantum attack for non-3GPP access, see clause 10.2, as the security of non-3GPP access relies on IPsec.

10.5 IMT-2020 core network

10.5.1 Within a PLMN

1) Authentication

To resist quantum attack, authentication based on NDS/IP is recommended to apply the same strategy introduced in clause 10.2.

2) Authorization

Quantum-safe keyed hash functions, such as HMAC-SHA-256, as well as quantum-safe signature algorithms, is recommended to be deployed in OAuth 2.0 to ensure the integrity of the access token. For the strategy to transit to the quantum-safe cipher suites in TLS, see clause 10.2.

Quantum-safe signature algorithms is recommended to be deployed for JWS.

10.5.2 Inter-PLMNs

The method introduced in clause 10.2 is recommended to be applied to N32-c to prevent the quantum attacker from deriving the session keys. AES-GCM with a 256 bit key is recommended to be deployed in an N32 interface to ensure the confidentiality and integrity of communication between PLMNs.

Quantum-safe signature algorithms is recommended to be deployed instead of ECDSA for JWS.

Appendix I

Overview of IMT-2020 system

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

This appendix gives an overall description of an IMT-2020 system.

I.1 General architecture

The IMT-2020 system aims to provide a wide range of services with different performance requirements. The services provided in IMT-2020 networks can be classified into three categories according to 3GPP specifications: (1) eMBB supports higher data rates and higher user mobility than 4G/LTE; (2) mIoT provides massive machine-type communications; (3) URLLC supports mission critical services that require higher reliability and lower latency. The IMT-2020 system is to be a flexible platform enabling new business cases and integrating vertical industries, such as, automotive, manufacturing, energy, eHealth and entertainment. Moreover, the deployment and maintenance of the IMT-2020 system is to be easier compared to previous generations of mobile networks. To address these challenging requirements, the IMT-2020 system has introduced a number of innovative technologies, such as network slicing, NFV, the SDN, SBA and central unit/distributed unit (CU/DU) separation.

The general architecture of an IMT-2020 system, illustrated in Figure I.1, can be divided into: infrastructure layer; network layer; service layer; and management plane, according to the functionality.

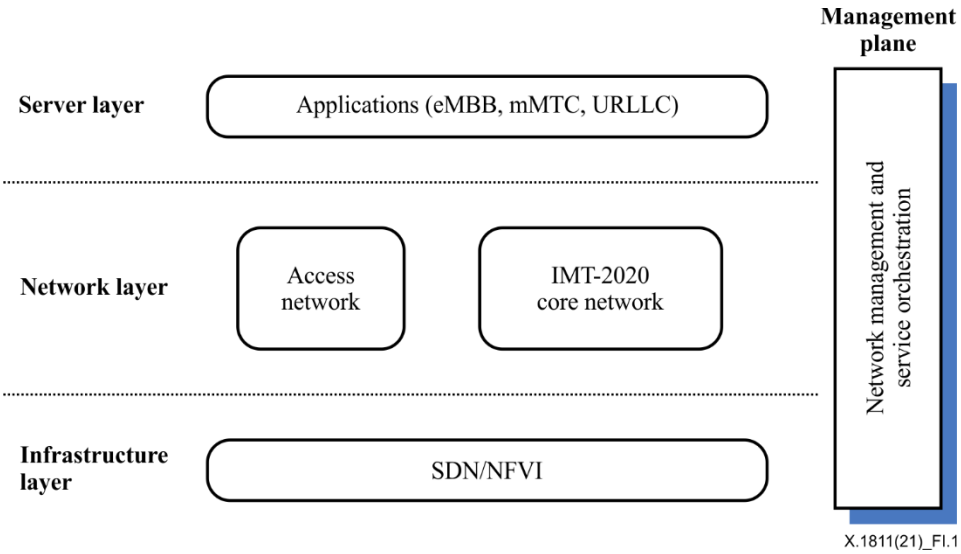

Figure I.1 – General architecture of the IMT-2020 system

– Infrastructure layer, encompassing the SDN and NFVI. The SDN is used to transport packets to the destination. Besides legacy transport technologies (e.g., multiprotocol label switching (MPLS)), the IMT-2020 system has introduced SDN technology for higher transport speed and easy adaptation to service requirements. NFVI is the common base for running VNFs.

– Network layer, composed of access and core networks. The former allows UE access to an IMT-2020 network anywhere. The latter is designed with an SBA in mind for extensibility and simplicity. It is made up of a number of NFs to support data connectivity and service deployment, such as the AUSF, AMF, and SMF.

– Service layer, consisting of the applications running on top of the IMT-2020 system, which may be eMBB applications, massive machine-type communication (mMTC) applications, and URLLC applications.
– Management plane, responsible for network management and service orchestration.

I.2 SDN

The basic principle of the SDN is that the data plane is decoupled from the control plane (CP), so that it can support dynamic programmability of network nodes in the process of data forwarding. The SDN controller makes the networking decisions and sends the resulting forwarding rules to the network nodes. This forwarding mechanism simplifies the realization of the network nodes and leads to enhanced data plane performance. The SDN architecture is depicted in Figure I.2.

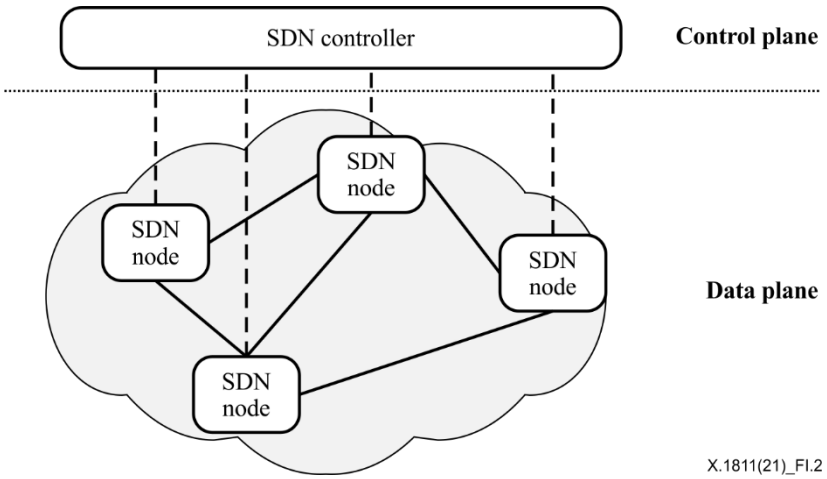

Figure I.2 – The SDN architecture

I.3 Access network

A UE can gain access to an IMT-2020 core network either in an untrusted non-3GPP access fashion or in a 3GPP access fashion, as shown in Figure I.3. The access network provides services related to the transmission of data over the radio interface.

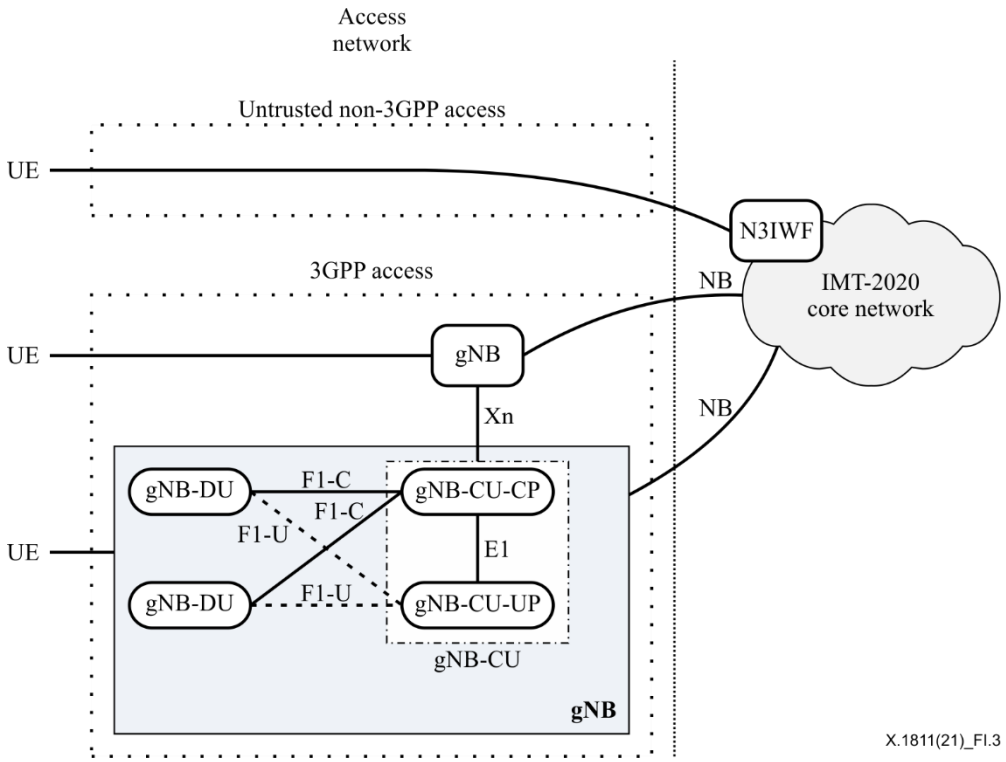

Figure I.3 – Access network

– **Untrusted non-3GPP access**

Untrusted non-3GPP access means that an access technology is not specified by 3GPP and is not trusted by the IMT-2020 core network, such as wireless local area network (WLAN) access. In this context, a UE connects to the IMT-2020 core network via an N3IWF.

– **3GPP access**

3GPP access is an access technology specified by 3GPP, i.e., next generation-radio access network (NG-RAN) technology in the IMT-2020 context. A UE can gain access to the IMT-2020 core network by using an NG interface via a flat gNB without CU/DU separation. An NG interface is a logical interface supporting the exchange CP information and UP information between the gNB and the IMT-2020 core network. For more flexible network deployment and lower costs, a gNB can be split into gNB-DU and gNB-CU. A gNB-CU is a logical node that carries out higher layer protocols, including the service data adaptation protocol (SDAP), radio resource control (RRC), and packet data convergence protocol (PDCP). A gNB-DU is a logical node that performs lower layer functions, including radio link control (RLC), medium access control (MAC) and physical layer functions.

Borrowed from the SDN concept, the gNB-CU can be further split into gNB-CU-CP and gNB-CU-UP. This would result in a functional decomposition of the radio access between user and CP entities. Such separation of CP and UP provides the flexibility to operate and manage complex networks, supporting different network topologies, resources and new service requirements.

A gNB-CU and the gNB-DU units are connected via an F1 logical interface, which can be distinguished between an F1-C interface for connecting the gNB-CU-CP and an F1-U interface for connecting the gNB-CU-UP. A gNB-CU-CP communicates with a gNB-CU-UP through an E1-interface.

I.4 Core network

The IMT-2020 core network is defined as an SBA, as shown in Figure I.4. A number of NFs have been defined in the SBA to serve different purposes. Each NF exposes a set of services called NF

service that is consumed by other authorized NFs. NFs query an NRF to discover and communicate with each other.

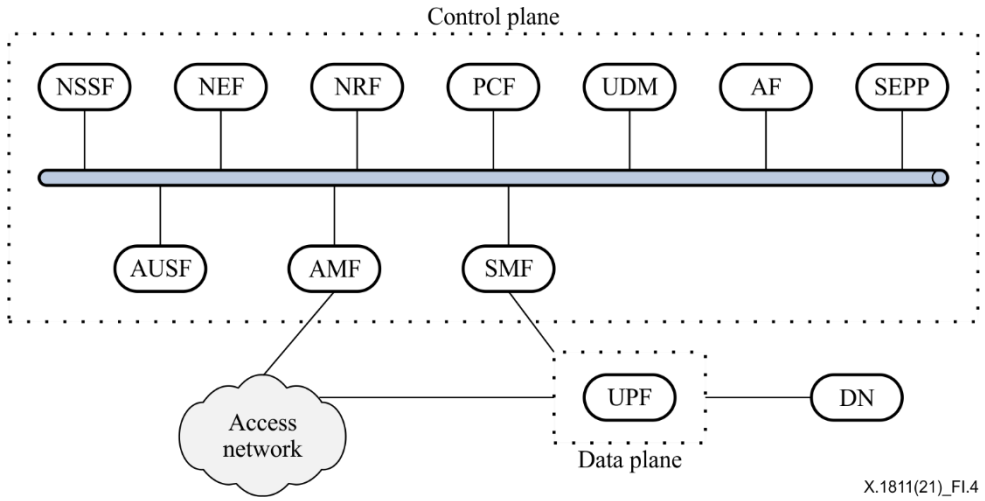

Figure I.4 – IMT-2020 core network

The IMT-2020 core network can be divided into the CP and UP.

– **Control plane**

  This plane provides network control services, including access, mobility, policy, exposure, legal intercept and charging-related control. The following NFs have been defined in the CP.

– **Network slice selection function** (NSSF), used to select the set of network slice instances serving the UE.

– **Network exposure function** (NEF), supporting exposure of capabilities and events. NFs expose capabilities and events to other NFs via the NEF. NF-exposed capabilities and events may be securely exposed for e.g., third party, application functions and edge computing.

– **NF repository function** (NRF), providing registration and discovery functions, so that NFs can discover and communicate with each other via APIs.

– **Policy control function** (PCF), supporting a unified policy framework to govern network behaviour.

– **Unified data management** (UDM), storing subscriber data and profiles. UDM is also used to generate the AVs for 3GPP AKA.

– **Application function** (AF), interacting with the 3GPP core network in order to provide services. The AF also provides information on the packet flow to the PCF.

– **Security edge protection proxy** (SEPP), a non-transparent proxy used to protect messages exchanged on inter-PLMN CP interfaces and hide the topology of the intra-PLMN network.

– **Authentication server function** (AUSF), handling authentication requests for both 3GPP access and non-3GPP access.

– **Access and mobility management function** (AMF), providing authentication, authorization and mobility management to UEs.

– **Session management function** (SMF), used for session management, e.g., session establishment, modification and release. The SMF also allocates IP addresses to UEs.

– **User plane**

User plane function (UPF) is the unique function defined for the UP. The UPF supports various operations and functionalities related to the UP packets, such as packet routing and forwarding, traffic handling, packet inspection and packet duplication.

The IMT-2020 core network is significantly different from the core network of previous generation mobile networks with the following features.

– **SBA,** whose services operate with finer granularity than in legacy networks and are loosely coupled with each other. This enables a short time to market for new services and greater flexibility for system updates.

– **Control plane and user plane separation**, allowing the UPF to be deployed in a place closer to the UE, so that these strict latency requirements from URLLC services can be met. Control plane and user plane separation also enables each plane resource to be scaled independently.

– **AMF and SMF separation**, allowing access and mobility management to be performed in a centralized manner. In contrast, the SMF can be located in a place where services need it.

– **NFV**, where the IMT-2020 core network assumes that NFs are implemented in a virtualized manner for better resource management and cost savings. An NFV that separates hardware and software makes the network more flexible and simpler by minimizing dependence on hardware constraints.

– **Network slice**, whose purpose is to support multiple service types on a common physical network infrastructure. It can provide customized end-to-end networks to meet different requirements. Each network slice may contain various NFs according to service requirements.

I.5 Management plane

The management plane is in charge of network management and service orchestration. In order to manage and monitor networks, the management plane connects to the access network, core network and SDN via an individual dedicated communication channel, as shown Figure I.5. Network management has at least the following functionalities: fault management (FM), performance management (PM), configuration management (CM) and trace management (TM). Besides these network management functions, the management of the network slice also needs the following functions: slice lifecycle management, slice capability management and network resource discovery. The service orchestration applies flexible resource control and monitoring mechanisms for the provision, management and re-optimization of network services.

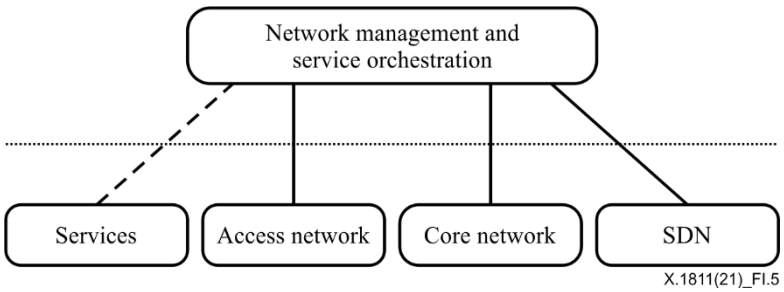

Figure I.5 – General management architecture

Appendix II

Quantum-safe asymmetric key cryptographic algorithms

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

This appendix lists the well-known quantum-safe asymmetric key cryptographic algorithms.

II.1 Lattice-based algorithms

Some lattice-based algorithms are:

– *N*th degree truncated polynomial ring (NTRU) [b-Hoffstein];
– Learning with errors (LWE) [b-Regev];
– Ring learning with errors (R-LWE) [b-Lyubashevsky];
– NewHope scheme [b-Alkim].

II.2 Hash-based algorithms

Some hash-based algorithms are:

– extended Merkle signature scheme (XMSS) [b-Buchmann];
– SPHINCS [b-Bernstein 2015];
– Leighton-Micali hash-based Signatures (LMS) [b-IRTF RFC 8554].

II.3 Code-based algorithms

Some code-based algorithms are:

– classic McEliece [b-McEliece];
– Niederreiter scheme [b-Dinh].

II.4 Multivariate algorithms

Some practical signature schemes based on multivariate algorithms are:

– Rainbow [b-Ding];
– Unbalanced oil and vinegar (UOV) [b-Kipnis].

II.5 NIST standardization of post quantum cryptography

On 20 December 2016, NIST announced the request for nominations for public-key post-quantum cryptographic algorithms. In the first round, NIST accepted 69 candidates, consisting of 20 digital signature schemes and 49 public-key encryption (PKE) or key encapsulation mechanisms (KEMs). On 30 January 2019, NIST selected as second round candidates the 26 algorithms listed in Table II.1, which include nine digital signature schemes, and 17 PKE and key-establishment schemes [b-NISTIR 8240].

Table II.1 – NIST second round algorithms

Classification	Problem base	Algorithm
Encryption/KEMs	Lattice-based	Crystals-Kyber
		FrodoKEM
		LAC
		NewHope

Table II.1 – NIST second round algorithms

Classification	Problem base	Algorithm
		NTRU
		NTRU Prime
		Round 5
		Saber
		Three Bears
	Code-based	Classic McEliece
		NTS-KEM
		BIKE
		HQC
		Rollo
		LEDAcrypt
		RQC
	Isogency-based	SIKE
Signature	Lattice-based	Crystals-Dilithium
		Falcon
		qTesla
	Multivariate-based	GeMSS
		LUOV
		MQDSS
		Rainbow
	Hash-based	Sphincs+
		Picnic

NIST intends to standardize post-quantum public-key algorithms for use in a wide variety of protocols, such as TLS, secure shell (SSH), Internet key exchange (IKE), IPsec and domain name system security extensions (DNSSEC) [b-NISTIR 8240].

NIST assesses the second round algorithms from both the security and performance perspective. NTRU encryption was invented in 1996, and its security has been reasonably well understood and scrutinized for decades. Moreover, NTRU encryption is standardized in [b-IEEE Std 1363.1]. Classic McEliece is based on [b-McEliece], which has not been broken, and is considered to be secure in a quantum world. In contrast, many other schemes have been released no more than 10 years ago. Thus, these schemes still need deep cryptanalysis by the cryptographic community in order to improve confidence in their security. In particular, SIKE, which originated from [b-Jao], relies on the problem of finding isogenies between supersingular elliptic curves, which has not been studied as much as some of the security problems associated with other candidates [b-NISTIR 8240].

Perfect forward secrecy means that past session keys will not be disclosed, even if the long-term key is exposed. This is a useful security property desired by widely used security protocols, such as IPsec and TLS. Of all the candidates, only SIKE and NewHope are able to support perfect forward secrecy.

The performance of the algorithms is measured in terms of the size of public keys, ciphertext and signatures, as well as the computation efficiency of encryption and decryption. PQC algorithms usually have much larger size of public keys, ciphertext, and signatures compared the classical public-key algorithms. The public-key size of candidates varies from 726 bytes to over 1 Mbyte

according to [b-NIST PQC]. The SIKE has the smallest public-key size, while the public-key size of classic McEliece and NTS-KEM is much larger than that of other schemes. However, classic McEliece and NTS-KEM can generate smaller cipher text than other schemes with a competitive encryption speed. The performance of SIKE seems to be an order of magnitude slower than many other candidates in spite of having the smallest public-key size. A trade-off between bandwidth efficiency and computation efficiency is therefore needed when selecting PQC algorithms.

In 2020, NIST plans to either select finalists for a final round or select a small number of candidates for standardization [b-NISTIR 8240]. This means that not merely one, but a set of PQC algorithms will be standardized. In the mobile environment, performance is of critical importance due to the precious wireless resources in air interface and limited computation capabilities in devices. The final standardized algorithms, which have smaller sizes of public keys and ciphertext, and competitive encryption speed, should be introduced into IMT-2020 systems.

Appendix III

Impact of quantum computing on common cryptographic algorithms

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

This appendix lists the impact of quantum computing on common cryptographic algorithms.

Table III.1 shows a summary of the impact of large-scale quantum computers on common cryptographic algorithms, such as RSA and the advanced encryption standard (AES).

It is not known how far these quantum advantages can be pushed, nor how wide is the gap between feasibility in the classical and quantum models [b-NISTIR 8105].

Table III.1 – Impact of quantum computers on commonly used cryptographic algorithms
[b-NISTIR Quantum report]

Cryptographic algorithm	type	use	impact
AES	Symmetric	Encryption	Large key sizes is needed
SHA-2, SHA-3	Hash	Hash function	Larger output is needed
RSA	Public key	Signature, key transport	No longer secure
ECDSA, ECDH	Public key	Signature, key exchange	No longer secure
DSA	Public key	Signature, key exchange	No longer secure

Appendix IV

Assessment criteria for quantum-safe cryptography

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

This appendix provides NIST assessment criteria for selecting the quantum-safe cryptography.

The submitted cryptographic algorithms will be assessed based on three aspects: security, cost, algorithm and implementation characteristics [b-NIST-Sub].

IV.1 Security

The security provided by a cryptographic scheme is the most important factor in the evaluation. Schemes will be judged on the following factors:

Applications of public-key cryptography: Post-quantum algorithms to its existing standards for digital signatures (FIPS 186) and key establishment (SP 800-56A, SP 800-56B) will be standardized. These are used in a wide variety of Internet protocols, such as TLS, SSH, IKE, IPsec, and DNSSEC. Schemes will be evaluated by the security they provide in these applications during the evaluation process. Claimed applications will be evaluated for their practical importance if this evaluation is necessary for deciding which algorithms to standardize.

Security definition for encryption/key-establishment: Post quantum algorithms for encryption or key establishment should be "semantically secure" with respect to adaptively chosen cryptographic attacks. This property is generally denoted *IND-CCA2* security in academic literature.

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted KEM and encryption schemes will be evaluated based on how well they appear to provide this property, when used as specified by the submitter. Submitters are not needed to provide a proof of security, although such proofs will be considered if they are available.

For the purpose of estimating security strengths, it may be assumed that the attacker has access to the decryptions of no more than 2^{64} chosen ciphertexts; however, attacks involving more ciphertexts may also be considered.

Security definition for ephemeral-only encryption/key-establishment: While chosen ciphertext security is necessary for many existing applications (for example, nominally ephemeral key exchange protocols that allow key caching), it is possible to implement a purely ephemeral key exchange protocol in such a way that only passive security is needed from the encryption or KEM primitive.

For these applications, post quantum algorithms for ephemeral-only encryption/key-establishment should be semantic security with respect to chosen plain text attacks. This property is commonly marked as *IND-CPA* security in the academic literature.

Submitted KEM and encryption schemes will be evaluated based on how well they appear to provide this property, when used as specified by the submitter. Submitters are not needed to provide a proof of security, although such proofs will be considered if they are available. Any security vulnerabilities that result from re-using a key should be fully explained.

Security definition for digital signatures: Post quantum algorithms for digital signature enable existentially unforgeable digital signatures with respect to an adaptive chosen message attack. This property is generally denoted *EUF-CMA security* in academic literature.

Submitted algorithms for digital signatures will be evaluated based on how well they appear to provide this property when used as specified by the submitter.

For the purpose of estimating security strengths, it may be assumed that the attacker has access to signatures for no more than 264 chosen messages.

Additional security properties: While the previously listed security definitions cover many of the attack scenarios that will be used in the evaluation of the submitted algorithms, there are several other properties that would be desirable:

One such property is perfect forward secrecy. While this property can be obtained through the use of standard encryption and signature functionalities, the cost of doing so may be prohibitive in some cases. In particular, public-key encryption schemes with a slow key generation algorithm, such as RSA, are typically considered unsuitable for perfect forward secrecy. This is a case where there is high corelation between the cost, and the practical security of an algorithm.

Another case where security and performance interact is resistance to side-channel attacks. Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks. We further note that optimized implementations that address side-channel attacks (e.g., constant-time implementations) are more meaningful than those which do not.

A third desirable property is resistance to multi-key attacks. Ideally an attacker should not gain an advantage by attacking multiple keys at once, whether the attacker's goal is to compromise a single key pair, or to compromise a large number of keys.

A final desirable, although ill-defined, property is resistance to misuse. Schemes should ideally not fail catastrophically due to isolated coding errors, random number generator malfunctions, nonce reuse, keypair reuse (for ephemeral-only encryption/key establishment), etc.

Other consideration factors: As public-key cryptography tends to contain subtle mathematical structure, it is very important that the mathematical structure be well understood in order to have confidence in the security of a cryptosystem. To assess this, a variety of factors will be considered. All other things being equal, simple schemes tend to be better understood than complex ones. Likewise, schemes whose design principles can be related to an established body of relevant research tend to be better understood than schemes that are completely new, or schemes that were designed by repeatedly patching older schemes that were proven vulnerable to cryptanalysis.

The clarity of the documentation of the scheme and the quality of the analysis provided by the submitter will be considered. Clear and thorough analysis will help to develop the quality and maturity of analysis by the wider community. Any security arguments or proofs provided by the submitter will be considered. While security proofs are generally based on unproven assumptions, they can often rule out common classes of attacks or relate the security of a new scheme to an older and better studied computational problem.

IV.2 Cost

The cost of a public-key cryptosystem can be measured on many different dimensions.

Public key, Ciphertext, and signature size: Schemes will be evaluated based on the sizes of the public keys, ciphertexts, and signatures that they produce. All of these may be important consideration factors for bandwidth-constrained applications or in Internet protocols that have a limited packet size. The importance of public-key size may vary depending on the application; if applications can cache public keys, or otherwise avoid transmitting them frequently, the size of the public key may be of lesser importance. In contrast, applications that seek to obtain perfect forward secrecy by transmitting a new public key at the beginning of every session are likely to benefit greatly from algorithms that use relatively small public keys.

Computational efficiency of public and private key operations: Schemes will also be evaluated based on the computational efficiency of the public key (encryption, encapsulation, and signature verification) and private key (decryption, decapsulation, and signing) operations. The computational cost of these operations will be evaluated both in hardware and software. The computational cost of both public and private key operations is likely to be important for almost all operations, but some

applications may be more sensitive to one or the other. For example, signing or decryption operations may be done by a computationally constrained device like a smartcard; or alternatively, a server dealing with a high volume of traffic may need to spend a significant fraction of its computational resources verifying client signatures.

Computational efficiency of key generation: Schemes will also be evaluated based on the computational efficiency of their key generation operations, where applicable. The most common scenario where key generation time is important is when a public-key encryption algorithm or a KEM is used to provide perfect forward secrecy. Nonetheless, it is possible that key generation times may also be important for digital signature schemes in some applications.

Decryption failures: Some public-key encryption algorithms and KEMs, even when correctly implemented, will occasionally produce ciphertexts that cannot be decrypted/decapsulated. For most applications, it is important that such decryption failures be rare or absent. For algorithms with decryption/decapsulation failures, submitters must provide the failure rate, as well as an analysis of the impact on security that these failures could cause. While applications can always obtain an acceptably low decryption failure rate by encrypting the same plaintext multiple times, and interactive protocols can simply restart when key establishment fails, these types of solutions have their own performance costs.

IV.3 Algorithm and implementation characteristics

Flexibility: Assuming good overall security and performance, schemes with greater flexibility will meet the needs of more users than less flexible schemes, and therefore, are preferable.

Some examples of "flexibility" may include (but are not limited to) the following:

1) The scheme can be modified to provide additional functionalities that extend beyond the minimum requirements of public-key encryption, KEM (key encapsulation mechanism), or digital signature (e.g., asynchronous or implicitly authenticated key exchange, etc.).
2) It is straightforward to customize the scheme's parameters to meet a range of security targets and performance goals.
3) The algorithms can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.
4) Implementations of the algorithms can be parallelized to achieve higher performance.
5) The scheme can be incorporated into existing protocols and applications, requiring as few changes as possible.

Simplicity: The scheme will be judged according to its relative design simplicity.

Adoption: Factors that might hinder or promote widespread adoption of an algorithm or implementation will be considered in the evaluation process, including, but not limited to, intellectual property covering an algorithm or implementation and the availability and terms of licenses to interested parties. Assurances made in the statements by the submitter(s) and any patent owner(s) will be considered, with a strong preference for submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination.

Bibliography

[b-ITU-T X.1196] Recommendation ITU-T X.1196 (2012), *Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment.*

[ITU-T X.1197] Recommendation ITU-T X.1197 (2019), *Guidelines on the selection of cryptographic algorithms for IPTV services, Amendment 1*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

[b-ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks.*

[b-ETSI 135 205] ETSI 135 205 V4.0.0 (2001), *Universal mobile telecommunications system (UMTS); LTE;3G security*; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General.

[b-ETSI 135 231] ETSI 135 231 V12.1.0 (2014), *Universal mobile telecommunications system (UMTS)*; LTE; Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification.

[b-ETSI GR QSC 004] ETSI GR QSC 004 V1.1.1 (2017), *Quantum-safe cryptography; Quantum-safe threat assessment*.

[b-ETSI GR QSC 006] ETSI GR QSC 006 V1.1.1 (2017), *Quantum-safe cryptography (QSC); Limits to quantum computing applied to symmetric key sizes*.

[b-ETSI GS NFV 002] ETSI GS NFV 002 V1.1.1 (2013). *Network functions virtualisation (NFV); Architectural framework*.

[b-ETSI GS NFV-SEC 012] ETSI GS NFV-SEC 012 V3.1.1 (2017), *Network functions virtualisation (NFV) release 3;Security; System architecture specification for execution of sensitive NFV components*.

[b-ETSI GS NFV-SEC 014] ETSI GS NFV-SEC 014 V3.1.1 (2018), *Network functions virtualisation (NFV) release 3; NFV security; Security specification for MANO components and reference points*.

[b-3GPP TS 33.210] 3GPP TS 33.210 V16.2.0 (2019), *3G security; Network domain security (NDS); IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220, V16.0.0 (2019), *Generic authentication architecture (GAA); generic bootstrapping architecture (GBA)*.

[b-3GPP TS 33.310] 3GPP TS 33.310 V16.2.0 (2019), *Network domain security (NDS); Authentication framework (AF).*

[b-3GPP TS 33.501] 3GPP TS 33.501, version 16.1.0 (2019), *System architecture for the 5G system.*

[b-3GPP TR 33.841] 3GPP TR 33.841 (2018), *Study on the support of 256-bit algorithms for 5G.*

[b-Häner] Häner, T., Roetteler, M., Svore, K.M. (2017). Factoring using 2*n* + 2 qubits with Toffoli based modular multiplication. *Quantum Information and Computation*, **18**(7-8), pp. 673-684.

[b-Hoffstein] Hoffstein, J., Pipher, J., Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem. In: Buhler, J.P. (editor), *Algorithmic number theory – ANTS 1998*, pp. 267-288. *Lecture Notes in Computer Science*, volume. 1423. Berlin: Springer.DOI: 10.1007/BFb0054868.

[b-IEEE Std 1363.1] IEEE Std 1363.1-2008, *IEEE Standard Specification for public key cryptographic techniques based on hard problems over lattices*.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-hashing for message authentication*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security architecture for the Internet protocol*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP encapsulating security payload (ESP)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS)*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5288] IETF RFC 5288 (2008), *AES Galois counter mode (GCM) cipher suites for TLS*.

[b-IETF RFC 5289] IETF RFC 5289 (2008), *TLS elliptic curve cipher suites with SHA-256/384 and AES Galois counter mode (GCM)*.

[b-IETF RFC 5869] IETF RFC 5869 (2010), *HMAC-based extract-and-expand key derivation function (HKDF)*.

[b-IETF RFC 6083] IETF RFC 6083 (2011), *Datagram transport layer security (DTLS) for stream control transmission protocol (SCTP)*.

[b-IETF RFC 6347] IETF RFC 6347 (2012), *Datagram transport layer security version 1.2*.

[b-IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 authorization framework*.

[b-IETF RFC 7296] IETF RFC 7296 (2014), *Internet key exchange protocol version 2 (IKEv2)*.

[b-IETF RFC 7515] IETF RFC 7515 (2015), *JSON web signature (JWS)*.

[b-IETF RFC 7516] IETF RFC 7516 (2015), *JSON web encryption (JWE)*.

[b-IETF RFC 7519] IETF RFC 7519 (2015), *JSON web token (JWT)*.

[b-IRTF RFC 8554] IRTF RFC 8554 (2019), *Leighton-Micali hash-based signatures*.

[b-ISO 7498-2] ISO 7498-2:1989, *Information Processing Systems* – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

[b-ISO/IEC TR 22417] ISO/IEC TR 22417:2017, *Information technology* – Internet of things (IoT) use cases.

[b-Ajtai] Ajtai, M. (1998). The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In: Vitter, J. (editor). *STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pp 10–19. New York, NY: Association for Computing Machinery. DOI: 10.1145/276698.276705.

[b-Alkim] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P. (2017). Post-quantum key exchange – A new hope, *Cryptology ePrint Archive*, Report 2015/1092. Available [viewed 2020-02-03] at: https://eprint.iacr.org/2015/1092 .

[b-Amy] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J. (2017). Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. In: Avanzi, R., Heys H. (editors). *Selected areas in cryptography, SAC 2016*, St. Johns, Canada, 2016, pp. 317-337. *Lecture Notes in Computer Science*, volume 10532. Cham: Springer. DOI: 10.1007/978-3-319-69453-5_18.

[b-Banchi] Banchi, L., Pancotti, N., Bose, S. (2016). Quantum gate learning in qubit networks: Toffoli gate without time-dependent control. *npj Quantum Information* **2**, 16019. DOI: 10.1038/npjqi.2016.19. Available [viewed 2020-02-02] at: https://www.nature.com/articles/npjqi201619#ref-link-section-82

[b-Bertoni] Betrtoni, G., Daemen, J., Peeters, M., Van Assche, G. *Keccak sponge function family main document*. Available at: https://keccak.team/obsolete/Keccak-main-1.1.pdf

[b-Bernstein 2009] Bernstein, D.J. (2009). Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? In: Workshop Record of SHARCS '09: Special-purpose Hardware for Attacking Cryptographic Systems. Available [viewed 2020-02-03] at: https://cr.yp.to/hash/collisioncost-20090517.pdf

[b-Bernstein 2015] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical stateless hash-based signatures. In: Oswald, E., Fischlin, M. (editors). *Advances in Cryptology – EUROCRYPT 2015*, pp. 368-397. *Lecture Notes in Computer Science*, volume 9056. Berlin: Springer. DOI: 10.1007/978-3-662-46800-5_15

[b-Buchmann] Buchmann, J., Dahmen, E., Hülsing, A. (2011). XMSS: A practical forward secure signature scheme based on minimal security assumptions. In: Yang, B.-Y. (editor). *Post-quantum cryptography*, pp. 117-129. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_8

[b-CSA] Cloud Security Alliance (2017), *Applied quantum-safe security: Quantum-resistant algorithms and quantum key distribution.* Available [viewed 2020-02-03] from: https://cloudsecurityalliance.org/download/applied-quantum-safe-security

[b-Dinh] Dinh, H., Moore, C., Russell, A. (2011). McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks. In: Rogaway, P. (editor). *Advances in cryptology – CRYPTO 2011*, pp. 761-779. *Lecture Notes in Computer Science*, volume 6841. Berlin: Springer. DOI: 10.1007/978-3-642-22792-9_43.

[b-Ding] Ding, J. Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (editors). *Applied Cryptography and Network Security, ACNS 2005*, pp. 164-175. *Lecture Notes in Computer Science*, volume 3531. Berlin: Springer. DOI: 10.1007/11496137_12.

[b-Fowler] Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, **86**, 032324. DOI: 10.1103/PhysRevA.86.032324. Available [viewed 2020-02-02] at: https://web.physics.ucsb.edu/~martinisgroup/papers/Fowler2012.pdf

[b-Garey] Garey, M.R. Johnson, D.S. (1979). *Computers and intractability: A guide to the theory of NP-completeness*. New York, NY: W.H. Freeman. 338 pp.

[b-Grassl] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In: Takagi T. (editor). *Post-quantum cryptography – PQCrypto 2016*, pp. 29-43. *Lecture Notes in Computer Science*, volume 9606. Cham: Springer. Available [viewed 2020-02-03] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/1512.04965-1.pdf

[b-Grover] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. In: *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp 212-219. New York, NY: Association for Computing Machinery. DOI: 10.1145/237814.237866.

[b-Jao] Jao, D., De Feo, L. (2011), Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B-Y. (editor). *Post-quantum cryptography*, pp 19-34. *Lecture Notes in Computer Science*, volume 7071. Berlin: Springer. DOI: 10.1007/978-3-642-25405-5_2.

[b-Kipnis] Kipnis, A., Patarin, J., Goubin, L. (1999), Unbalanced oil and vinegar signature schemes. In: Stern, J. (editor). *Advances in Cryptology – EUROCRYPT '99*. pp. 206-222. *Lecture Notes in Computer Science*, volume 1592. Berlin: Springer. DOI: 10.1007/3-540-48910-X_15.

[b-Lyubashevsky] Lyubashevsky, V., Peikert, C., Regev, O. (2013), On ideal lattices and learning with errors over rings. *Journal of the ACM*, **60**(6), Article No. 43. DOI: 10.1145/2535925.

[b-McEliece] McEliece, R.J. (1978), A *public-key cryptosystem based on algebraic coding theory*. In: *DSN Progress Report*, No. 44, pp. 114–116. Bibcode:1978DSNPR. Available [viewed 2020-02-03] at: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF

[b-Moody] Moody, D. (2019), *NIST status update on elliptic curves and post-quantum crypto*. Gaithersberg, MA: National Institute of Standards and Technology. 20 pp. Available [viewed 2020-02-03] at: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Status-Update-on-Elliptic-Curves-and-Post-Qua/images-media/moody-dustin-threshold-crypto-workshop-March-2019.pdf

[b-Moses] Moses, T. (2009), *Quantum computing and cryptography – Their impact on cryptographic practice*. Minneapolis, MN: Entrust Inc. 12 pp. Available [viewed 2020-02-03] at: https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf

[b-NASEM] National Academies of Sciences, Engineering, and Medicine (2018). *Quantum computing: Progress and prospects*. Washington, DC: National Academies Press. 272 pp. DOI: 10.17226/25196.

[b-NIST FIPS 186-4] National Institute of Standards and Technology Federal Information Processing Standard 186-4 (2013), *Digital signature standard (DSS)*. DOI: 10.6028/NIST.FIPS.186-4. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[b-NIST FIPS 197] National Institute of Standards and Technology Federal Information Processing Standard 197 (2001), *Specification for the advanced encryption standard (AES)*. Available [viewed 2020-02-14] at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[b-NISTIR 8105] National Institute of Standards and Technology Internal Report 8105 (2016), *Report on* post-*quantum cryptography*. Gaithersberg, MA: National Institute of Standards and Technology. 15 pp. DOI: 10.6028/NIST.IR.8105. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[b-NISTIR 8240] National Institute of Standards and Technology Internal Report 8240 (2019), *Status* report on the first round of *the NIST post-quantum cryptography standardization process*. Gaithersberg, MA: National Institute of Standards and Technology. 27 pp. DOI: 10.6028/NIST.IR.8240. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf

[b-NIST PQC] National Institute of Standards and Technology Post-Quantum Cryptography: Round 2 – algorithm comparison. Available [viewed 2020-02-14] at:http://hdc.amongbytes.com/post/20190130-pqc-round2/

[b-NIST SP 800-38B] National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for block cipher modes of operation: The CMAC mode for authentication*. Gaithersberg, MA: National Institute of Standards and Technology. 21 pp. DOI: 10.6028/NIST.SP.800-38B. Available [viewed 2020-02-03] at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[b-NIST SP 800-67] National Institute of Standards and Technology Special Publication 800-67 Rev. 2 (2017), *Recommendation for the triple data encryption algorithm (TDEA) block cipher.* DOI: 10.6028/NIST.SP.800-67r2.

[b-NIST-Sub] National Institute of Standards and Technology. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Available [viewed 2020-03-20] at : https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[b-ONF TR-511] Open Network Foundation Technical Recommendation 511 (2015), *Principles and practices for securing software-defined networks*. Available [viewed 2020-02-02] at: https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf

[b-QC1] IBM's processor pushes quantum computing closer to 'supremacy' available at: https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/

[b-QC2] Practical Quantum Computers, available at: https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/

[b-Regev] Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In: *STOC'05 Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. pp. 84-93. New York, NY: Association for Computing Machinery. DOI: 10.1145/1060590.1060603

[b-Roetteler] Roetteler, M., Naehrig, M., Krysta M. Svore, K.M., Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. In: Takagi T., Peyrin T. (editors). *Advances in Cryptology – ASIACRYPT 2017*, pp. 241-270. *Lecture Notes in Computer Science*, volume 10625. Cham: Springer. DOI: 10.1007/978-3-319-70697-9_9. Available [viewed 2020-02-02] at: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/09/1706.06752.pdf

[b-Schneier] Schneier, B. (1994). The Blowfish encryption algorithm. *Dr. Dobb's Journal*, 19(4), pp. 38-40. Available [viewed 2020-02-03] from: https://www.drdobbs.com/security/the-blowfish-encryption-algorithm/184409216

[b-Shor 1997] Shor, P.W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), pp. 1484–1509. DOI: 10.1137/S0097539795293172

[b-Shor 1999] Shor, P.W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev*. 41(2), pp. 303-332. DOI: 10.1137/S0036144598347011.

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