INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-TD1526R1

STUDY GROUP 17

Original: English

Question(s): 6/17 Geneva, 29 August – 7 September 2018

TD

Source: Editors

Title: New baseline for draft Recommendation X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems

Purpose: Proposal

Contact: Fuwen LIU
China Mobile
China
Tel: +86 18811463269
Fax: +86 10 63135376
Email: liufuwen@chinamobile.com

Contact: Zhiyuan HU
Nokia Shanghai Bell
China
Email: zhiyuan.1.hu@nokia-sbell.com

Contact: Zhaoji Lin
ZTE
P.R.China
E-mail: lin.zhaoji@zte.com.cn

Keywords: 5G system; Quantum computer; Symmetric algorithm; Asymmetric algorithm; Quantum-safe algorithm

Abstract: The joint session meeting of Q2/17 and Q6/17, carefully reviewed and discussed C359, C389, and made the following agreement:
1) C359, C389 are accepted.
2) A new TD is created based on C359 and C389 for a new baseline text for draft Recommendation ITU-T X.5GSec-q. The revised text includes improvements as followings:
- add overview of 5G system in clause 7.
- add appendix A: Overview of 5G system

Annex 1:

Draft Recommendation of ITU-T X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems

Annex 1

Security guidelines for applying quantum-safe algorithms in 5G systems

Summary

The 5G 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 innovation technologies have been developed in the 5G system, such as network slicing, software defined network, virtualized network function, CU/DU separation. Security measures are the basis to ensure the normal operation of the 5G system. Besides the use of the symmetric cryptographic algorithms, asymmetric cryptographic algorithms have been deployed in the 5G system.

A large-scale quantum computer raises security concerns to present widely used the symmetric and asymmetric cryptographic algorithms. The currently used asymmetric cryptographic algorithms provide no security any more in the quantum computing era, while the symmetric cryptographic algorithms have to double their key lengths to resist against the quantum computing attacks. For this, quantum-safe cryptographic algorithms are highly desired to be deployed in the 5G system.

In this Recommendation, firstly, the 5G system and its security architecture will be shortly surveyed, respectively. Then the threats to 5G systems due to the quantum computers will be assessed. The quantum-safe algorithms will be briefly reviewed but their details are not specified in this Recommendation. The security guidelines will provide a high level recommendation to adapt quantum-safe algorithms to 5G systems. This Recommendation is intended to give a whole picture to apply the quantum-safe symmetric and asymmetric algorithms to 5G system, as well as align the security levels between quantum-safe symmetric algorithms and quantum-safe asymmetric algorithms.

Keywords

5G system; Quantum computer; Symmetric algorithm; Asymmetric algorithm; Quantum-safe algorithm

Table of Contents

1 Scope 6

2 References 6

3 Definitions 6

4 Abbreviations and acronyms 6

5. Conventions 7

6. Overview 8

7. Overview of 5G system 8

8. Security architecture of 5G systems 9

9. Security assessment on 5G systems when commercial quantum computers are available 9
- 9.1 Threats to conventional cryptographic algorithms 9
- 9.2 Impacts on 5G systems 9

10. Quantum-safe cryptographic algorithms 9
- 10.1 Quantum-safe symmetric key algorithms 10
- 10.2 Quantum-safe asymmetric key algorithms 10
  - 10.2.1 Lattice-based algorithms 10
  - 10.2.2 Hash-based algorithms 10
  - 10.2.3 Code-based algorithms 10
  - 10.2.4 Multivariate algorithms 10

11. Usage of the quantum-safe cryptographic algorithms in 5G systems 11
- 11.1 Quantum-safe symmetric cryptographic algorithms 11
- 11.2 Quantum-safe asymmetric cryptographic algorithms 11

Appendix A 12
- A.1 General architecture 12
- A.2 SDN 13
- A.3 Access network 13
- A.4 Core network 15
- A.5 Management Plane 16

Appendix B 18
- B.1 Lattice-based algorithms 18
- B.2 Hash-based algorithms 18
- B.3 Code-based algorithms 18
- B.4 Multivariate algorithms 18

Bibliography 19

Introduction

Draft Recommandation ITU-T X.5GSec-q

Security guidelines for applying quantum-safe algorithms in 5G systems

1 Scope

This Recommendation is Security guidelines for applying quantum-safe algorithms in 5G systems. This recommendation covers:

- Introduction of the security architecture of 5G systems
- Security assessment on 5G systems when commercial quantum computers are available.
- Specify the usage of quantum-safe algorithms in 5G 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.yyy] Recommendation ITU-T X.yyy (date), *Title*.

3 Definitions

<Check in ITU-T Terms and definitions database under http://www.itu.int/sancho/index.htm if the term is not already defined in another recommendation. It could be more consistent to refer to such a definition rather than redefined it>

3.1 Terms defined elsewhere

<Normally, terms defined elsewhere will simply refer to the defining document. In certain cases, it may be desirable to quote the definition to allow for a stand-alone document>

This Recommendation uses the following terms defined elsewhere:

3.1.1 <Term 1> [Reference]: <optional quoted definition>.

3.1.2 <Term 2> [Reference]: <optional quoted definition>.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF Application Function

AUSF	Authentication Server Function
AMF	Access and Mobility management Function
CU/DU	Central Unit / Distributed Unit
eMBB	enhanced Mobile Broadband
MAC	Medium Access Control
mIoT	massive Internet of Things
MPLS	Multiprotocol Label Switching
N3IWF	Non-3GPP InterWorking Function
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualization
NRF	NF Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
RLC	Radio Link Control
RRC	Radio Resource Control
PLMN	Public Land Mobile Network
SBA	Service Based Architecture
SDAP	Service Data Adaptation Protocol
SDN	Software Defined Network
SMF	Session Management function
UDM	Unified Data Management
UPF	User plane function
URLLC	Ultra-Reliable and Low-Latency Communications

[Editor note]: Only the abbreviations and acronyms used in the following clauses could be listed above.

< Others to be added>

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 fifth generation of mobile communication technology (5G) is positioned to meet the business needs of the year 2020 and beyond. Security architecture is the key stone to enable the normal operation of a 5G network. In 4G/LTE, mere symmetric algorithms are utilized to protect the signalling data and user data. In contrast, besides the use of the symmetric algorithms, asymmetric algorithms are introduced in 5G systems to protect the subscriber identifiers, as well as to enhance the security of the session keys in the case that the long-term key is disclosed.

Recently the IBM had announced the 50 qubits quantum computer. This breakthrough in the development of quantum computers has broken the original anticipation that quantum computers can be on the market in 20 years. The new report estimated that large-scale quantum computers will be available in 10 years.

Quantum computers will affect the symmetric algorithms and asymmetric algorithms to a different degree. Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength, whereas many commonly used asymmetric algorithms, such as RSA, DSA and ECC, will offer no security.

There is a high desire to study how to protect the communications in 5G systems by using quantum-safe algorithms. This is because it is most likely that the commercial quantum computers are available within the lifecycle of 5G systems. Currently, the key length of the symmetric algorithms specified for 5G systems is 128 bits. 3GPP has just initiated a study item to research how to apply 256 bit key length symmetric algorithms to 5G systems. However, there is no organization to study how to apply the quantum-safe asymmetric algorithms to 5G systems till now. Some adapting measures have to be taken when quantum-safe cryptographic algorithms are used in 5G systems since these algorithms have a larger key length than the classical cryptographic algorithms. Moreover, there is a need to study how the keys of different size coexist in 5G systems since it is impossible to replace all the classical algorithms with quantum-safe algorithms overnight. A transition to quantum-safe cryptography in 5G 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 5G systems due to the quantum computers will be assessed. The quantum-safe algorithms will be briefly reviewed but their details are not specified in this work item. The security guidelines will provide a high level recommendation to adapt quantum-safe algorithms to 5G systems. This Recommendation is intended to give a whole picture to apply the quantum-safe symmetric and asymmetric algorithms to 5G system, as well as align the security levels between quantum-safe symmetric algorithms and quantum-safe asymmetric algorithms.

7. Overview of 5G system

[Editor note]: This clause only gives an overview of 5G system. The detailed definition and background information used in the following clause could refer to the Appendix A.

The 5G system aims at providing a wide range of services with different performance requirements. The services provided in 5G networks can be classified into Enhanced Mobile Broadband (eMBB), Massive Internet of Things (mIoT), ultra-reliable and low-latency communications (URLLC).

The 5G system introduces a number of innovation technologies, such as network slicing, network function virtualization (NFV), software defined network (SDN), service based architecture (SBA). These technologies make 5G system to be a flexible platform enabling new business cases and integrating vertical industries. On the other side, they make the security of the 5G system to be much more complicated compared to the previous generations of mobile networks.

8. Security architecture of 5G systems

Editor's note: the following security functions of 5G systems will be briefly introduced in this section:

1) Authentication
2) Key hierarchy
3) Subscription identifier privacy
4) NAS security mechanisms
5) RRC security
6) UP security
7) Security of Service Based Interfaces

9. Security assessment on 5G systems when commercial quantum computers are available

The threats to conventional cryptographic algorithms due to the availability of quantum computers are first introduced. Then the impacts on 5G systems raised by quantum computers will be analyzed. In the following descriptions, the security level alignment between quantum-safe symmetric algorithms and quantum-safe asymmetric algorithms are considered.

9.1 Threats to conventional cryptographic algorithms

1) Symmetric cryptographic algorithms
2) Asymmetric cryptographic algorithms

9.2 Impacts on 5G systems

1) Authentication
2) Key hierarchy
3) Subscription identifier privacy
4) NAS security mechanisms
5) RRC security
6) UP security
7) Security of Service Based Interfaces

10. Quantum-safe cryptographic algorithms

Quantum computing introduces a completely new computing paradigm. This will impact 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.

As for symmetric key algorithms, [b-Entrust] shows that quantum computing effectively halves the number of bits of key strength for any symmetric key algorithm, and also shows that quantum

computers can run algorithms (e.g., Grover's [b-Grover96]) 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 Diffie-Hellman, the effect of quantum computing on them is thought to be quite serious. Quantum computers can run algorithms (e.g., Shor's [b-Shor97]) that break all the 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-Entrust].

10.1 Quantum-safe symmetric key algorithms

It is widely believed that basic symmetric cryptosystems such as block ciphers (e.g., AES) or hash functions (e.g., SHA2 or SHA3) are quantum-safe algorithms [b-CSA]. The advent of the quantum computer will require an increase in the key size (and a doubling of the bit number). [b-CSA] shows that the current recommended key size of 256 bits is considered as safe, even against Grover's algorithm.

Symmetric key algorithms, such as AES, SNOW 3G and ZUC, are widely used for mobile communication networks.

10.2 Quantum-safe asymmetric key algorithms

Although quantum computers can run algorithms that break the current public-key systems (e.g., RSA and ECC) in trivial amounts of time, there are many important classes of cryptographic systems beyond RSA and ECC that are secure against an attack by a quantum computer and described as below.

10.2.1 Lattice-based algorithms

Lattice-based algorithms are based on the constructions of cryptographic primitives that involve lattices, either in the construction itself or in the security proof.

[b-CSA] shows that Lattice-based algorithms can provide digital signature, public/private key encryption and key agreement. Some of Lattice-based algorithms are listed in Appendix I.1.

10.2.2 Hash-based algorithms

[b-CSA] shows that Hash-based algorithms are used for digital signatures constructed using hash functions. Some of hash-based algorithms are listed in Appendix B.2.

10.2.3 Code-based algorithms

Code-based algorithms rely on error-correcting codes.

[b-CSA] shows that Code-based algorithms can provide digital signature, public/private key encryption and key agreement. Some of Code-based algorithms are listed in Appendix I.3.

10.2.4 Multivariate algorithms

Multivariate algorithms are based on the difficulty of solving systems of multivariate polynomials over finite fields.

[b-CSA] shows that Multivariate algorithms can provide digital signature and public/private key encryption. Some practical signature schemes based on Multivariate algorithms are listed in Appendix B.4.

11. Usage of the quantum-safe cryptographic algorithms in 5G systems

11.1 Quantum-safe symmetric cryptographic algorithms

1) Authentication
2) Key hierarchy
3) Subscription identifier privacy
4) NAS security mechanisms
5) RRC security
6) UP security
7) Security of Service Based Interfaces

11.2 Quantum-safe asymmetric cryptographic algorithms

1) Authentication
2) Subscription identifier privacy
3) Security of Service Based Interfaces

Appendix A

Overview of 5G system

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

A.1 General architecture

The 5G system aims at providing a wide range of services with different performance requirements. The services provided in 5G networks can be classified into three categories according to 3GPP specifications: (1) Enhanced Mobile Broadband (eMBB) supports higher data rates and higher user mobility than the Fourth Generation of Mobile Communication technology/Long Term Evaluation network (4G/LTE);(2) Massive Internet of Things (mIoT) provides massive machine type communications; (3) ultra-reliable and low-latency communications (URLLC) supports the mission critical services which require higher reliability and lower latency. The 5G 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 5G system is to be easier compared to the previous generations of mobile networks. To address these challenging requirements, the 5G system has introduced a number of innovation technologies, such as network slicing, network function virtualization (NFV), software defined network (SDN), service based architecture (SBA), and central unit / distributed unit (CU/DU) separation.

A general architecture of the 5G system is illustrated in Figure A-1, which can be divided into transport layer, network layer, service layer, and management plane according to the functionality.

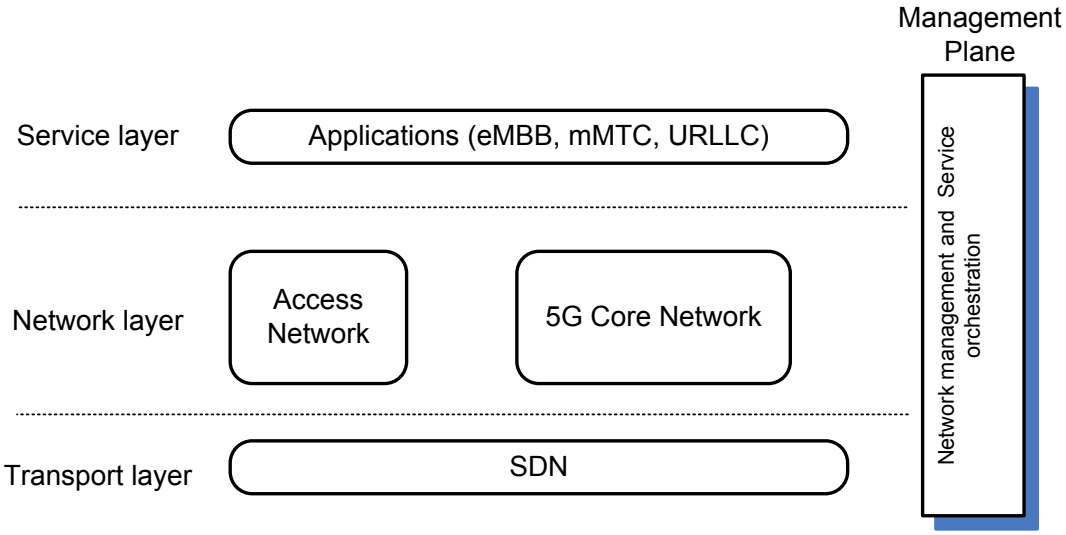

Figure A-1. General architecture of the 5G system

- Transport layer: It is used to transport packets to the destination. Besides legacy transport technologies (e.g. MPLS), the 5G system has introduced SDN technology for higher transport speed and easy adaption to the service requirements.
- Network layer: It is composed of access network and core network. The former allows UE access to 5G network anywhere. The latter is designed with a service-based architecture in mind for extensibility, and simplicity. It is made up of a number of network functions to support data connectivity and service deployment, such as authentication server function (AUSF), access and mobility management function (AMF), and session management function (SMF).
- Service layer: It consists of the applications running on the top of the 5G system, which may be eMBB applications, mMTC applications, and URLLC applications.

- Management plane: It is responsible for the network management and service orchestration.

A.2 SDN

The basic principle of SDN is that the data plane is decoupled from the control plane so that it can support dynamic programmability of network nodes in the process of data forwarding. 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 A-2.

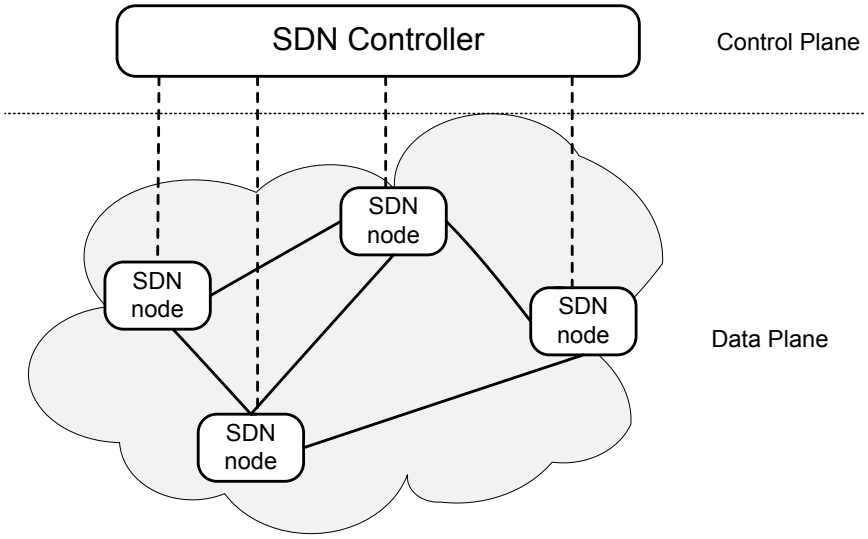

Figure A-2. SDN architecture

A.3 Access network

A UE can gain access to 5G core network either in an untrusted non-3GPP access fashion or in a 3GPP access fashion, as shown in Figure 3. The access network provides services related to the transmission of data over the radio interface.

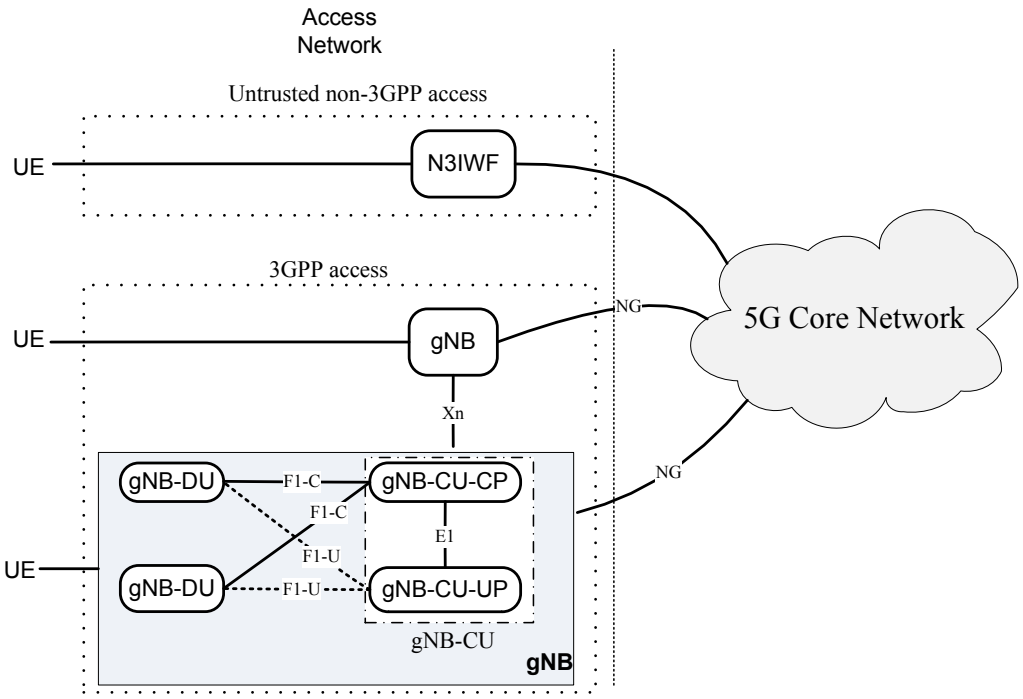

Figure A-3. Access network

- **Untrusted non-3GPP access**

  The untrusted non-3GPP access means that an access technology is not specified by 3GPP, and is not trusted by the 5G core network, such as WLAN access. In this context, a UE connects to the 5G core network via a Non-3GPP InterWorking Function (N3IWF).

- **3GPP access**

  3GPP access is an access technology specified by 3GPP, i.e. NG-RAN technology in the 5G context. A UE can gain access to the 5G core network by using NG interface via a flat gNB without CU-DU separation. A NG interface is a logical interface supporting the exchange control plane information and user plane information between the gNB and the 5G core network. For more flexible network deployment and lower costs, a gNB can be split into gNB-DU (Distributed Unit) and gNB-CU (Central-Unit). A gNB-CU is a logical node that carries out the higher layer protocols, including 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 SDN concept, the gNB-CU can further be split into gNB-CU-CP (control plane) and gNB-CU-UP (user plane). This would result in a functional decomposition of the radio access between user and control plane entities. Such separation of control plane and user plane 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 F1 logical interface, which can be distinguished between F1-C interface for connecting the gNB-CU-CP and F1-U interface for connecting the gNB-CU-UP. A gNB-CU-CP communicates with a gNB-CU-UP through E1-interface.

A.4 Core network

The 5G core network is defined as a service-based architecture (SBA) as shown in Figure A-4. A number of Network Functions (NFs) have been defined in the SBA architecture to serve the different purposes. Each Network Function (NF) exposes a set of services called NF service that is consumed by other authorized NFs. NFs query an NF repository function (NRF) to discover and communicate each other.

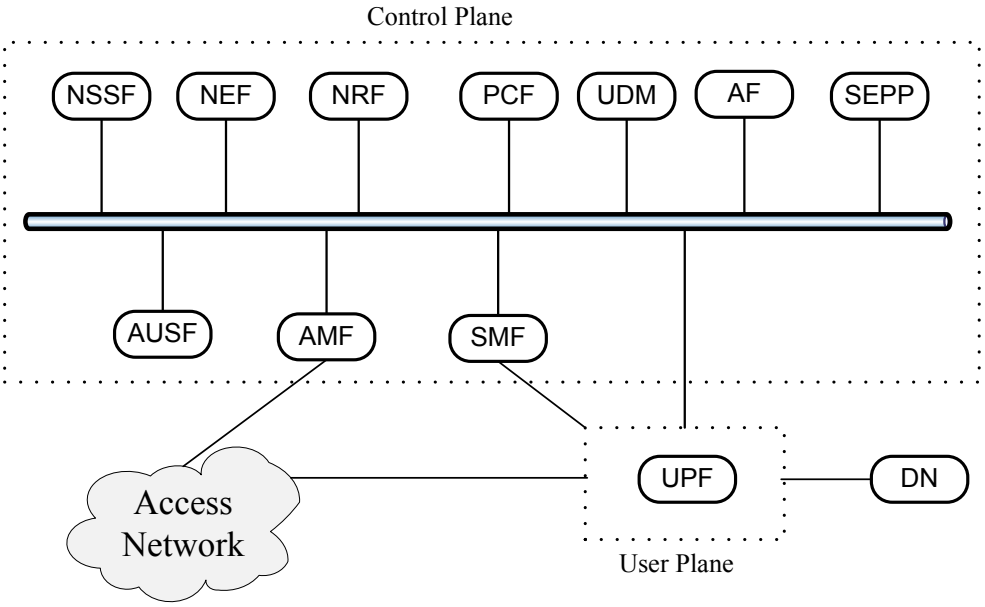

Figure A-4. 5G core network

The 5G core network can be divided into the control plane and user plane.

- **Control plane**

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

- **Network Slice Selection Function** (NSSF): It is used to select the set of network slice instances serving the UE.
- **Network Exposure Function** (NEF): It supports exposure of capabilities and events. NFs expose capabilities and events to other NFs via NEF. NF exposed capabilities and events may be securely exposed for e.g. 3rd party, Application Functions, Edge Computing.
- **NF Repository Function** (NRF): It provides registration and discovery functions so that NFs can discover and communicate each other via application programming interfaces (APIs)
- **Policy Control Function** (PCF): It supports unified policy framework to govern network behavior.
- **Unified Data Management** (UDM): It stores subscriber data and profile. It is also used to generate the authentication vectors for 3GPP AKA.
- **Application Function** (AF): It interacts with the 3GPP Core Network in order to provide services. It also provides information on the packet flow to PCF.
- **Security Edge Protection Proxy** (SEPP): It is a non-transparent proxy used to protect messages exchanged on inter-PLMN control plane interfaces and hide the topology of the intra-PLMN network.

- **Authentication server function** (AUSF): It handles authentication requests for both, 3GPP access and non-3GPP access.
- **Access and Mobility Management function** (AMF): It provides authentication, authorization, and mobility management to UEs.
- **Session Management function** (SMF): It is used for session management e.g. session establishment, modify and release. It also allocates IP addresses to UEs.

- **User plane**

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

The 5G core network is significantly different from the core network of previous generation mobile networks with following features:

- **Service-based architecture**: Services operate with finer granularity than in legacy networks and are loosely-coupled with each other. This enables short time to the market for new services and greater flexibility for system updates.
- **Control plane and user plane separation**: This allows the UPF to be deployed in the place where are more close to UEs so that these strict latency requirements from URLLC services are possible to be met. It also enables that each plane resource is scaled independently.
- **AMF and SMF separation**: The access and mobility management can be performed in a centralized manner. In contrast, SMF can be located in the place where services need.
- **Network Function Virtualization (NFV)**: The 5G core network assumes that NFs are implemented in a virtualization manner for better resource management and cost savings. NFV that separates hardware and software makes the network more flexible and simple by minimizing dependence on hardware constraints.
- **Network Slice**: It is purposed 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 the service requirements.

A.5 Management Plane

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

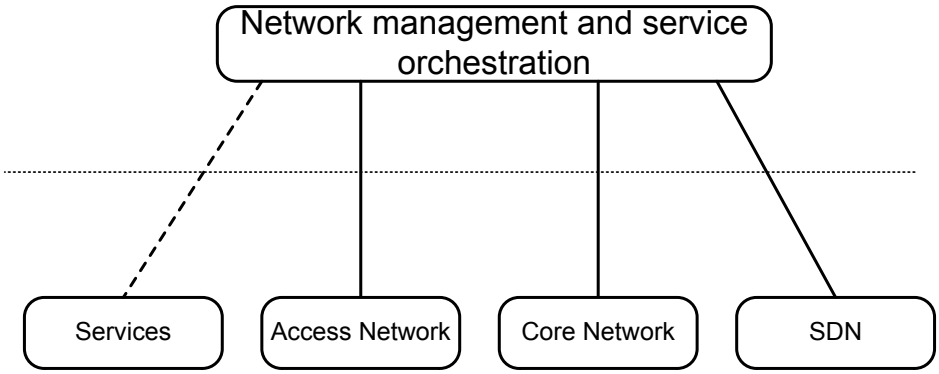

Figure A-5. General Management architecture

Appendix B

Quantum-safe asymmetric key cryptographic algorithms

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

B.1 Lattice-based algorithms

Some of Lattice-based algorithms are:

- NTRU [b-NTRU]
- LWE (Learning With Errors) [b-LWE]
- R-LWE (Ring Learning With Errors) [b-RLWE]
- New Hope Scheme [b-NewHope]

B.2 Hash-based algorithms

Some of hash-based algorithms are:

- XMSS [b-XMSS]
- SPHINX [b-SPHINCS15]
- LMSS [b-LMSS]

B.3 Code-based algorithms

Some of Code-based algorithms are:

- Classic McEliece [b-McEliece]
- Niederreiter Scheme [b- Niederreiter]

B.4 Multivariate algorithms

Some practical signature schemes based on Multivariate algorithms are:

- Rainbow [b- Rainbow]
- UOV [b-UOV]

[Editor Note]: quantum-safe asymmetric key algorithms in Appendix B will be updated according to the industry research, e.g., NIST project Post-Quantum Cryptography.

Bibliography

[b-CSA] Applied Quantum-Safe Security: *Quantum-Resistant Algorithms and Quantum Key Distribution*, 2017, available at : https://cloudsecurityalliance.org/download/applied-quantum-safe-security

[b-Entrust] T. Moses, *Quantum Computing and Cryptography – Their impact on cryptographic practice*, Entrust Inc., January 2009.

[b-Grover96] Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*. *STOC* '96 *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp 212-219). New York, NY: ACM Publications.

[b-LMSS] D. McGrew, M. Curcio, S. Fluhrer, *Hash-Based Signatures*, IETF RFC draft, available at: https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/

[b-LWE] Regev, O. (2005). *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*. STOC'05 Proceedings of the thirty-seventh annual ACM symposium on Theory of computing (pp 84-93). New York, NY: ACM Publications.

[b-McEliece] McEliece, Robert J. (1978). *A Public-Key Cryptosystem Based On Algebraic Coding Theory*". DSN Progress Report. 44: 114–116. Bibcode:1978DSNPR.

[b-NewHope] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe, *Post-quantum key exchange - a new hope*, https://eprint.iacr.org/2015/1092, 2017.

[b- Niederreiter] D. Hang, M. Cristopher, R. Alexander and R. Philip, *McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks*, Advances in cryptology—CRYPTO, Lecture Notes in Computer Science, p. 761–779, 2011

[b-NTRU] Hoffstein, J., Pipher, J., & Silverman, J.H. (1998). *NTRU: A ring-based public key cryptosystem*. In: Buhler, J.P. (Ed.), *Algorithmic Number Theory* (pp. 267-288). Lecture Notes in Computer Science, Vol. 1423. Springer Berlin Heidelberg

[b-QC1] *Practical Quantum Computers*,

available at: https://www.technologyreview.com/s/603495/10-breakthrough-technologies-2017-practical-quantum-computers/

[b-QC2] *IBM's processor pushes quantum computing closer to 'supremacy'*

available at: https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/

[b-ETSI QSC] ETSI TC Cyber/QSC reports,

available at: http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

[b-SDN] Open Network Foundation, Software-Defined Networking: The New Norm for Networks 2012.

available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[b- Rainbow] J. Ding and D. Schmidt, Rainbow, *a new multivariable polynomial signature scheme*, ACNS, Lecture Notes in Computer Science, vol. 3531, pp. 164-175, 2005.

[b-RLWE] Lyubashevsky, V., Peikert, C., & Regev, O. (2013). *On Ideal Lattices and Learning with Errors over Rings*. Journal of the ACM (JACM), 60 (6), Article No. 43

[b-Shor97] 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

[b-SPHINCS15] 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. (Eds.) Advances in Cryptology—EUROCRYPT 2015 (pp. 368-397). Lecture Notes in Computer Science, Vol. 9056. Springer Berlin Heidelberg

[b-UOV] A. Kipnis, J. Patarin and L. Goubin, *Unbalanced oil and vinegar schemes*, in EUROCRYPT, Lecture Notes in Computer Science, 1999.

[b-XMSS] Buchmann, J., Dahmen, E., & Hülsing, A. (2011). *XMSS: A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions*. In: Yang, B.-Y. (Ed.) Post-Quantum Cryptography (pp. 117-129) Lecture Notes in Computer Science, Vol. 7071. Springer Berlin Heidelberg.

[b-3GPP TS 33.501] 3GPP TS 33.501 (2018), *System Architecture for the 5G System*.

[b-3GPP TR 28.801] 3GPP TR 28.801, *Telecommunication management; Study on management and orchestration of network slicing for next generation network.*

[b-3GPP TS 38.300] 3GPP TS 38.300, *NR; Overall description; Stage-2.*

[b-3GPP TS 38.401] 3GPP TS 38.401, *NG-RAN; Architecture description.*

[b-3GPP TS 33.501] 3GPP TS 33.501 (2018), *Security Architecture and Procedures for 5G System*.

[b-3GPP TR 33.899] 3GPP TR 33.899 (2017), *Study on the security aspects of the next generation system.*

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