Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1811

(04/2021)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des réseaux IMT-2020

Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020

Recommandation UIT-T X.1811

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DES RÉSEAUX IMT-2020	**X.1800–X.1819**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1811

Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020

Résumé

La Recommandation UIT-T X.1811 identifie les menaces que l'informatique quantique fait peser sur les systèmes des Télécommunications mobiles internationales (IMT) sur la base d'une évaluation du niveau de sécurité des algorithmes cryptographiques actuellement utilisés. Elle passe brièvement en revue les algorithmes à l'épreuve des attaques quantiques, de type symétrique et de type asymétrique, et énonce des lignes directrices relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020.

Historique

Edition	Recommandation	Approbation	Commission d'études*
1.0	UIT-T X.1811	30-04-2021	11.1002/1000/14454

Mots clés

Système 5G, algorithme asymétrique, système IMT-2020, ordinateur quantique, algorithme résistant aux attaques quantiques, algorithme symétrique.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

Les systèmes de Télécommunications mobiles internationales 2020 (IMT-2020), devraient prendre en charge un large éventail de services avec des exigences diverses en termes de qualité de fonctionnement, afin de constituer une société entièrement connectée. Pour atteindre cet objectif ambitieux, un certain nombre de technologies innovantes ont été élaborées dans les systèmes IMT-2020, comme le découpage de réseau, les réseaux pilotés par logiciel, les fonctions de réseau virtualisées et la séparation unité centrale/unité répartie (CU/DU). Les mesures de sécurité sont essentielles pour garantir le fonctionnement normal des systèmes IMT-2020. En plus de l'utilisation d'algorithmes de chiffrement symétriques, des algorithmes asymétriques ont été déployés dans les systèmes IMT-2020.

Un ordinateur quantique très puissant pose des problèmes de sécurité aux algorithmes de chiffrement symétriques et asymétriques largement utilisés actuellement. Les algorithmes asymétriques ne garantissent plus la sécurité à l'ère de l'informatique quantique. Quant aux algorithmes de chiffrement symétriques, ils doivent doubler la longueur de leurs clés pour résister aux attaques par informatique quantique. C'est pourquoi il est vivement souhaitable de déployer des algorithmes de chiffrement résistant aux attaques quantiques dans les systèmes IMT-2020.

La présente Recommandation présente brièvement les systèmes IMT-2020 et leur architecture de sécurité, évalue les menaces que représentent les ordinateurs quantiques pour ces systèmes et décrit brièvement les algorithmes résistant aux attaques quantiques sans les préciser. Des lignes directrices relatives à la sécurité feront l'objet d'une Recommandation de haut niveau, afin d'adapter les algorithmes résistant aux attaques quantiques aux systèmes IMT-2020. La présente Recommandation a vocation à fournir des lignes directrices, afin d'appliquer aux systèmes IMT-2020 des algorithmes symétriques et asymétriques résistant aux attaques quantiques, ainsi que d'aligner les niveaux de sécurité entre les algorithmes symétriques et asymétriques résistant aux attaques quantiques.

Recommandation UIT-T X.1811

Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020

1 Domaine d'application

La présente Recommandation contient:

- une introduction à l'architecture de sécurité des systèmes de Télécommunications mobiles internationales (IMT-2020);
- une évaluation de la sécurité des systèmes IMT-2020 lorsque des ordinateurs quantiques sont disponibles sur le marché;
- une spécification de l'utilisation d'algorithmes résistant aux attaques quantiques dans les systèmes IMT-2020.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[UIT-T X.1038] Recommandation UIT-T X.1038 (2016), *Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 authentification [b-UIT-T Y.2014]: processus consistant à établir l'identité correcte d'une entité avec un degré de confiance prescrit. L'entité à authentifier peut être un utilisateur, un abonné, un environnement de rattachement ou un réseau de desserte.

3.1.2 protocole d'authentification [b-UIT-T X.1254]: séquence définie de messages entre une entité et un contrôleur, qui permet à celui-ci d'authentifier l'entité.

3.1.3 autorisation [b-ISO 7498-2]: attribution de droits, comprenant l'autorisation d'accès sur la base de droits d'accès.

3.1.4 disponibilité [UIT-T X.800]: propriété d'être accessible et utilisable sur demande par une entité autorisée.

3.1.5 justificatif d'identité [b-UIT-T X.1252]: ensemble de données présentées comme preuve d'une identité et/ou d'une habilitation déclarée.

3.1.6 confidentialité [UIT-T X.800]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

3.1.7 intégrité des données [UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.8 respect de la vie privée [UIT-T X.800]: droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées et stockées, et sur les personnes par lesquelles et auxquelles ces informations peuvent être divulguées.

3.1.9 hiérarchie des clés [b-UIT X.1196]: structure arborescente qui représente la relation entre les différentes clés. Dans une hiérarchie des clés, un nœud représente une clé utilisée pour calculer les clés représentées par les nœuds descendants. Une clé ne peut avoir qu'un ascendant, mais peut avoir de multiples nœuds descendants.

3.1.10 virtualisation des fonctions de réseau; NFV [b-ISO/CEI TR 22417]: technologie qui permet de créer des subdivisions de réseau isolées de manière logique sur des réseaux physiques partagés de telle sorte que des collections hétérogènes de plusieurs réseaux virtuels peuvent coexister simultanément sur les réseaux partagés.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

4G	quatrième génération
AES	norme de chiffrement perfectionné (*advanced encryption standard*)
AES-CBC	norme de chiffrement perfectionné-enchaînement de blocs de chiffrement (*advanced encryption standard-cipher blocker chaining*)
AES-GCM	norme de chiffrement perfectionné-mode Galois compteur (*advanced encryption standard-Galois counter mode*)
AES-GMAC	norme de chiffrement perfectionné-code d'authentification de message Galois (*advanced encryption standard-Galois message authentication code*)
AF	fonction d'application (*application function*)
AKA	authentification et concordance de clés (*authentication and key agreement*)
AMF	fonction de gestion d'accès et de mobilité (*access and mobility management function*)
API	interface de programmation d'application (*application programming interface*)
ARPF	fonction de consignation et de traitement de justificatif d'authentification (*authentication credential repository and processing function*)
AS	strate accès (*access stratum*)
AUSF	fonction de serveur d'authentification (*authentication server function*)
AV	vecteur d'authentification (*authentication vector*)
CEK	clé de chiffrement de contenu (*content encryption key*)
CM	gestion de la configuration (*configuration management)*
CP	plan de commande (*control plane*)
CU/DU	unité centrale/unité répartie (*central unit/distributed unit*)
DH	Diffie-Hellman
DHE	mode éphémère Diffie-Hellman (*Ephemeral Diffie-Hellman*)

DNSSec	extensions de sécurité du système des noms de domaine (*domain name system security extensions*)
DSA	algorithme de signature numérique (*digital signature algorithm*)
DTLS	sécurité de la couche transport en mode datagramme (*datagram transport layer security*)
EAP	protocole d'authentification extensible (*extensible authentication protocol*)
ECC	cryptographie à courbe elliptique (*elliptic curve cryptography*)
ECDH	courbe elliptique Diffie-Hellman (*elliptic curve Diffie-Hellman*)
ECDHE	courbe elliptique Diffie-Hellman éphémère (*elliptic curve Diffie-Hellman ephemeral*)
ECDLP	problème du logarithme discret sur les courbes elliptiques (*elliptic curve discrete-log problem*)
ECDSA	algorithme de signature numérique à courbe elliptique (*elliptic curve digital signature algorithm)*
ECIES	système de chiffrement intégré à courbe elliptique (*elliptic curve integrated encryption scheme*)
ECP	plan sécant étendu (*extended cutting plane*)
eMBB	large bande mobile évolué (*enhanced mobile broadband*)
ESP	données utiles pour la sécurité d'encapsulation (*encapsulating security payload*)
FM	gestion des défaillances (*fault management*)
GKDF	fonction de calcul de clé générique (*generic key derivation function*)
gNB	nœud B NR
GUTI	identificateur temporaire unique à l'échelle mondiale (*globally unique temporary identifier*)
HMAC	code d'authentification de message par hachage (*hash-based message authentication code*)
HKDF	fonction de calcul de clé d'extraction et d'expansion HMAC (*HMAC-based extract-and-expand key derivation function*)
ICV	valeur de contrôle d'intégrité (*integrity check value*)
IPsec	sécurité du protocole Internet (*Internet protocol security*)
IKE	échange de clés Internet (*Internet key exchange*)
IKEv2	échange de clés Internet version 2 (*Internet key exchange version 2*)
IMT-2020	Télécommunications mobiles internationales-2020
IP	protocole Internet (*Internet protocol*)
IPX	échange IP (*IP exchange)*
JOSE	signature et chiffrement des objets en JavaScript (*Javascript object signing and encryption*)
JSON	notation des objets en JavaScript (*JavaScript object notation*)
JWE	chiffrement web JSON (*JSON web encryption*)
JWS	signature web JSON (*JSON web signature*)

KDF	fonction de calcul de clé (*key derivation function*)
KEM	mécanisme d'encapsulation de la clé (*key encapsulation mechanism*)
LTE	évolution à long terme (*long term evolution*)
LWE	apprentissage avec erreurs (*learning with errors*)
MAC	code d'authentification de message (*message authentication code*)
mIoT	Internet des objets massif (*massive Internet of Things*)
mMTC	communications massives de type machine (*massive machine-type communication*)
MNO	opérateur de réseau mobile (*mobile network operator*)
MODP	exponentiation modulaire (*modular exponential*)
MPLS	commutation multiprotocole par étiquette (*multiprotocol label switching*)
N3IWF	fonction d'interfonctionnement non 3GPP (*non-3GPP interworking function*)
NAS	strate hors accès (*non-access stratum*)
NDS	sécurité du domaine réseau (*network domain security*)
NEF	fonction d'exposition de réseau (*network exposure function*)
NF	fonction de réseau (*network function*)
NFV	virtualisation des fonctions de réseau (*network function virtualization*)
NFVI	infrastructure de virtualisation des fonctions de réseau (*network function virtualization infrastructure*)
NG-RAN	réseau d'accès radioélectrique de prochaine génération (*next generation-radio Access network*)
NP	non déterministe polynomial (*non-deterministic polynomial time*)
NRF	fonction de référentiel NF (*NF repository function*)
NSSF	fonction de sélection de tranche de réseau (*network slice selection function*)
NTRU	anneau de polynômes tronqués au degré n (*Nth degree truncated polynomial ring*)
PCF	fonction de contrôle des politiques (*policy control function*)
PDCP	protocole de convergence de données en mode paquet (*packet data convergence protocol*)
PKI	infrastructure de clé publique (*public-key infrastructure*)
PKE	chiffrement par clé publique (*public-key encryption*)
PM	gestion de la qualité de fonctionnement (*performance management*)
PRF	fonction pseudo-aléatoire (*pseudo-random function*)
PSK	clé pré-partagée (*pre-shared key*)
RLC	commande de liaison radioélectrique (*radio link control*)
R-LWE	apprentissage en anneau avec erreurs (*ring learning with errors*)
RRC	contrôle des ressources radioélectriques (*radio resource control*)
RSA	Rivest, Shamir et Adelman
RMTP	réseau mobile terrestre public

PQC	cryptographie post-quantique (*post-quantum cryptography*)
SBA	architecture fondée sur les services (*service-based architecture*)
SDAP	protocole d'adaptation des données de service (*service data adaptation protocol*)
SDN	réseau piloté par logiciel (*software-defined network*)
SEAF	fonction ancre de sécurité (*security anchor function*)
SEPP	proxy de protection pour la sécurité en périphérie de réseau (*security edge protection proxy*)
SHA	algorithme de hachage sécurisé (*secure hash algorithm*)
SIDF	fonction de suppression du masquage de l'identificateur d'abonnement (*subscription identifier de-concealing function*)
SIDH	isogénie supersingulière Diffie-Hellman (*supersingular-isogeny Diffie–Hellman*)
SIKE	encapsulation de clé à isogénie supersingulière (*supersingular isogeny key encapsulation*)
SMF	fonction de gestion de session (*session management function*)
SSH	connecteur sécurisé (*secure shell)*
SUCI	identificateur masqué d'abonnement (*subscription concealed identifier*)
SUPI	identificateur permanent d'abonnement (*subscription permanent identifier*)
SVP	problème du plus court vecteur (*shortest vector problem*)
TLS	sécurité dans la couche transport (*transport layer security*)
TM	gestion de trace (*trace management*)
UDM	gestion de données unifiée (*unified data management*)
UDR	répertoire des données d'utilisateur (*user data repository*)
UE	équipement d'utilisateur (*user equipment*)
UOV	mélange non équilibré d'huile et de vinaigre (*unbalanced oil and vinegar*)
UP	plan utilisateur (*user plane*)
UPF	fonction de plan utilisateur (*user plane function*)
URLLC	communications ultra-fiables présentant un faible temps de latence (*ultra-reliable and low-latency communication*)
USIM	module d'identité d'abonné universel (*universal subscriber identity module*)
VNF	fonction de réseau virtuelle (*virtual network function*)
WLAN	réseau local sans fil (*wireless local area network*)
XMSS	système de signature Merkle étendu (*extended Merkle signature scheme*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**il est interdit**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Ces mots n'impliquent pas que la mise en œuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau/le fournisseur de service. Ils signifient plutôt que le fabricant peut incorporer la caractéristique à titre facultatif et revendiquer néanmoins la conformité avec la spécification.

6 Vue d'ensemble

Les technologies de communication mobiles IMT-2020 sont à même de répondre aux besoins opérationnels à compter de 2020 et au-delà. L'architecture de sécurité est essentielle pour permettre le fonctionnement normal d'un réseau IMT-2020. Dans les réseaux 4G/LTE, seuls des algorithmes symétriques sont utilisés pour protéger les données de signalisation et d'utilisateur. En plus de ce type d'algorithmes, les systèmes IMT-2020 mettent en œuvre des algorithmes asymétriques pour protéger non seulement les identificateurs d'abonné, mais aussi les communications entre les opérateurs MNO.

Récemment (septembre 2020), IBM a présenté son ordinateur quantique d'une puissance de 50 qubits [b-QC1]. Cette incroyable avancée vient contredire les prédictions initiales selon lesquelles les ordinateurs quantiques très puissants arriveraient sur le marché dans 20 ans. Selon les estimations figurant dans le nouveau rapport [b-QC2], leur disponibilité d'ici à 10 ans est aujourd'hui réaliste.

La sécurité des algorithmes de chiffrement par clé publique dépend de la difficulté des problèmes de calcul à résoudre, comme la factorisation entière ou le problème du logarithme discret dans différents groupes. Il est démontré que les ordinateurs quantiques peuvent résoudre efficacement chacun de ces problèmes [b-Shor 1997], rendant ainsi inopérants tous les cryptosystèmes à clé publique fondés sur ces hypothèses. Ainsi, un ordinateur quantique suffisamment puissant constituera une menace pour de nombreuses formes de cryptosystèmes modernes, tels que l'échange de clés, le chiffrement et l'authentification numérique.

Les ordinateurs quantiques affecteront le niveau de sécurité des algorithmes dans des degrés différents selon que les algorithmes sont symétriques ou asymétriques. Le niveau de sécurité des algorithmes symétriques sera divisé par deux, par exemple, le niveau de sécurité d'un algorithme AES avec des clés de 128 bits donnant un niveau de 128 bits sera ramené à 64 bits, tandis que les algorithmes de chiffrement fréquemment utilisé, comme les algorithmes RSA et ECC n'offriront aucune sécurité.

Un système IMT-2020 a vocation à fournir un large éventail de services ayant des exigences différentes en termes de qualité de fonctionnement. Les services fournis dans les réseaux IMT-2020 peuvent être classés en trois catégories, à savoir le large bande mobile évolué (eMBB), l'Internet des objets massif (mIoT) et les communications ultra-fiables présentant un faible temps de latence (URLLC).

Les systèmes IMT-2020 introduisent un certain nombre de technologies innovantes, comme le découpage de réseau, la virtualisation des fonctions de réseau (NFV), les réseaux pilotés par logiciel (SDN) et l'architecture fondée sur les services (SBA). Grâce à ces technologies, les systèmes IMT-2020 sont une plate-forme souple permettant de nouveaux types de mise en œuvre et intégrant les secteurs verticaux. En revanche, ces technologies compliquent considérablement l'architecture de sécurité des systèmes IMT-2020 par rapport à celle des précédentes générations de réseaux mobiles.

L'étude de la manière de protéger les communications dans les systèmes IMT-2020 grâce à l'utilisation d'algorithmes à l'épreuve des attaques quantiques suscite un très vif intérêt, et ce car des ordinateurs quantiques seront probablement disponibles sur le marché avant que les systèmes IMT-2020 arrivent au bout de leur cycle de vie. Actuellement, la longueur des clés pour les algorithmes symétriques indiqués pour les systèmes IMT-2020 est de 128 bits. Le 3GPP vient de commencer des travaux de recherche sur la manière d'appliquer des algorithmes symétriques avec

une longueur de clés de 256 bits aux systèmes 5G [b-3GPP TR 33.841]. En revanche, rien n'a encore été mis en place pour étudier comment appliquer aux systèmes IMT-2020 des algorithmes asymétriques résistant aux attaques quantiques. Certaines adaptations doivent être faites lorsque des algorithmes de chiffrement résistant aux attaques quantiques sont utilisés dans des systèmes IMT-2020, étant donné que les clés correspondantes sont plus longues que celles utilisées dans le cas du chiffrement classique. De plus, il est nécessaire d'étudier comment des clés de tailles différentes coexistent dans des systèmes IMT-2020, étant donné qu'il est impossible de remplacer rapidement tous les algorithmes classiques par des algorithmes résistant aux attaques quantiques. Il convient d'étudier sans attendre le passage à un chiffrement résistant aux attaques quantiques dans les systèmes IMT-2020, afin que les informations qui pourraient être compromises ultérieurement par la cryptoanalyse quantique ne soient plus sensibles.

La présente Recommandation évalue les menaces que représentent les ordinateurs quantiques pour les systèmes IMT-2020 et passe rapidement en revue les algorithmes résistant aux attaques quantiques sans les préciser. Les lignes directrices relatives à la sécurité préconisent, à haut niveau, d'adapter aux systèmes IMT-2020 les algorithmes résistant aux attaques quantiques. La présente Recommandation fournit les lignes directrices détaillées, afin d'appliquer aux systèmes IMT-2020 des algorithmes symétriques et asymétriques résistant aux attaques quantiques, ainsi que d'aligner les niveaux de sécurité entre les algorithmes symétriques et asymétriques résistant aux attaques quantiques.

7 Introduction aux composants de sécurité des systèmes IMT-2020

Les paragraphes ci-après donnent des informations générales sur les composants de sécurité des systèmes IMT-2020, qui ont été indiqués dans le cadre de l'UIT-T, du 3 GPP, de l'ETSI, de l'IETF, etc.

Un système de communication devrait être capable de fournir certains des services de sécurité ci-après afin de garantir la sécurité du système ou de la transmission des données [UIT-T X.800]: contrôle d'accès (autorisation), authentification, respect de la vie privée, confidentialité, intégrité des données, non-répudiation et disponibilité.

Les services de sécurité pourraient être assurés à l'aide de systèmes cryptographiques ou non cryptographiques. La présente Recommandation porte sur ce premier type de systèmes, puisqu'elle analyse l'application d'algorithmes cryptographiques quantiques aux systèmes IMT-2020.

Conformément à l'architecture des systèmes IMT-2020 présentée dans l'Appendice I, l'architecture de sécurité des systèmes IMT-2020 peut être décrite en trois couches: la couche infrastructure, la couche réseau et le plan de gestion.

7.1 Sécurité de la couche infrastructure

La couche infrastructure est la base commune pour la prise en charge de la couche supérieure dans un système IMT-2020, qui comprend le réseau SDN et la couche de l'infrastructure de virtualisation des fonctions de réseau (NFVI)

7.1.1 Sécurité des réseaux SDN

La technologie SDN est utilisée pour la fourniture des données dans les systèmes IMT-2020, car elle offre une gestion dynamique et souple des flux de trafic. L'architecture de sécurité des réseaux SDN est indiquée dans la publication [UIT-T X.1038] et est présentée de manière simple dans la Figure 1.

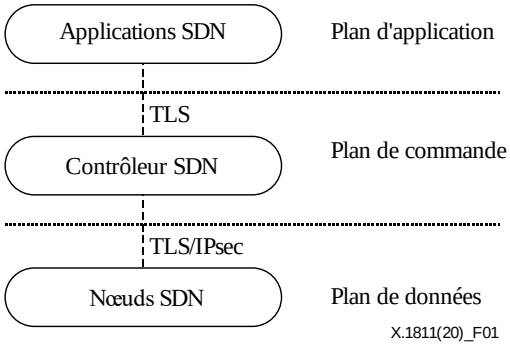

Figure 1 – Architecture de sécurité des réseaux SDN

La publication [UIT-T X.1038] indique les recommandations ci-après concernant les algorithmes de chiffrement et les protocoles.

Il est recommandé de déployer le protocole de sécurité de la couche transport (TLS), [b-IETF RFC 5246] dans l'interface entre l'application SDN et le contrôleur SDN. Sur la base du protocole TLS, l'application SDN et le contrôleur SDN s'authentifient mutuellement et conviennent de la clé de session; en outre, la confidentialité des données et l'intégrité des données dans l'interface application-commande sont assurées.

Il est recommandé de déployer le protocole TLS [b-IETF RFC 5246] ou les protocoles IPSec ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]) dans l'interface entre le contrôleur SDN et le nœud SDN. Sur la base du protocole TLS ou IPsec, le nœud SDN et le contrôleur SDN s'authentifient mutuellement et conviennent de la clé de session; en outre, la confidentialité des données et l'intégrité des données dans l'interface commande-nœud sont assurées.

Les mécanismes d'authentification pourraient être fondés sur une clé PSK [b-IETF RFC 4279] [b-IETF RFC 4306] ou un certificat [b-IETF RFC 4306] et [b-IETF RFC 5246]. Des algorithmes RSA [b-ONF TR-511] ou des algorithmes de signature numérique peuvent être appliqués dans le cadre d'une authentification fondée sur un certificat. Le protocole d'échange de clés DH ou le protocole d'échange de clés ECDH peut être mis en œuvre dans le contexte du protocole TLS ou des protocoles IPsec pour convenir de la clé partagée entre les deux entités.

Les algorithmes de chiffrement AES [b-NIST FIPS 197], Blowfish [b-Schneier] ou 3DES [b-NIST SP 800-67] pourraient être utilisés pour le chiffrement des données. Les algorithmes de chiffrement utilisés pour les mécanismes assurant l'intégrité des données pourraient être le code d'authentification de message (MAC) [b-IETF RFC 2104], le code d'authentification de message par hachage (HMAC) [b-IETF RFC 2104] ou la signature numérique [b-NIST FIPS 186-4].

7.1.2 Sécurité de la couche NFVI

La couche NFVI prend en charge l'exécution des fonctions de réseau virtuelles (VNF), dont la structure est décrite dans la Figure 2.

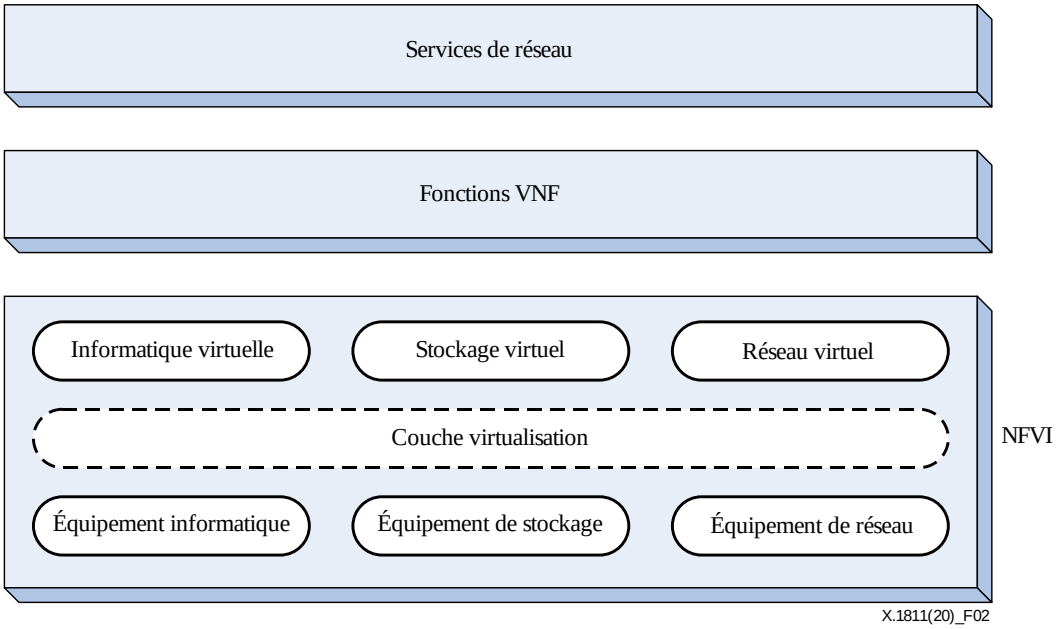

Figure 2 – Structure NFVI (adaptée de la Figure 1 de la publication [b-ETSI GS NFV 002])

Conformément à la publication [b-ETSI GS NFV-SEC 012], l'infrastructure NFVI prend en charge les fonctions de sécurité ci-après pour garantir la sécurité des fonctions VNF exécutées au-dessus: connexion sécurisée, contrôle d'accès et de confinement au niveau du système d'exploitation, contrôles et alarmes physiques, contrôle d'authentification, contrôles d'accès, sécurité des communications, attestation, enclaves d'exécution par l'équipement, racine de confiance fondée sur l'équipement, stockage à auto-chiffrement, accès direct à la mémoire, modules de sécurité matérielle et protection et vérification de l'intégrité logicielle. Pour ce faire, l'infrastructure NFVI doit mettre en œuvre les algorithmes de chiffrement [b-ETSI GS NFV-SEC 012] suivants:

1) Algorithmes de hachage: SHA-256, SHA-384, AES128-GMAC, HMAC-SHA128, HMAC-SHA256, HMAC-SHA384.
2) Algorithmes de chiffrement: AES-CBC-128, AES-GCM-128 (valeur ICV de 16 octets), AES-CBC-256, AES-GCM-256 (valeur ICV de 16 octets).
3) Signature: RSA 2048, RSA 3072, RSA 4096, ECDSA-256 (secp256r1), ECDSA-384 (secp384r1).
4) Infrastructure de clé publique (PKI): RSA 2048, RSA 3072, RSA 4096, id-ecPublicKey (secp256r1).
5) Échange de clés: groupe DH 14 (MODP 2 048 bits), groupe DH 19 (groupe ECP aléatoire 256 bits), groupe DH 20 (groupe ECP aléatoire 384 bits), ECDHE secp256r1 (P-256), groupes DHE d'au moins 2048 bits.
6) Fonction pseudo aléatoire (PRF): PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384.

7.2 Sécurité de la couche réseau

7.2.1 Sécurité du réseau d'accès

La sécurité du réseau d'accès [b-3GPP TS 33.501] est destinée à garantir que l'équipement UE authentifié est capable d'obtenir l'accès à un réseau IMT-2020, la communication entre l'équipement UE et le réseau IMT-2020 pourrait être protégée d'une manière qui serait choisie conformément à la politique de sécurité de l'opérateur MNO.

L'architecture de sécurité du réseau d'accès IMT-2020 est décrite dans la Figure 3 et peut être décrite comme suit. L'équipement UE essaie d'accéder au réseau avec une identité attribuée temporairement

à une identité permanente masquée avant d'invoquer le protocole AKA. L'équipement UE et le réseau s'authentifient mutuellement et conviennent d'une clé de session en exécutant le protocole AKA. L'équipement UE et le réseau calculent un ensemble de clés fondées sur la clé de session. Sur la base de ces clés, l'intégrité et la protection de la réponse pour les messages de signalisation NAS échangés entre l'équipement UE et la fonction AMF sont obligatoires, tandis que la protection de la confidentialité de ces messages est facultative; l'intégrité et la protection de la réponse pour les messages de signalisation AS échangés entre l'équipement UE et le nœud gNB sont obligatoires, tandis que la protection de la confidentialité de ces messages est optionnelle. La confidentialité et la protection de l'intégrité des données d'utilisateurs dans le plan utilisateur entre l'équipement UE et le nœud gNB sont facultatives. On utilise un tunnel IPsec pour protéger la communication entre l'équipement UE et la fonction N3IWF dans le cas d'un accès non 3GPP. Étant donné que les unités gNB-DU et gNB-CU pourraient être déployées à des endroits différents, on applique la sécurité NDS/IP pour protéger l'interface F1 située entre ces deux unités. De même, l'interface E1 entre l'unité gNB-CU du plan de commande et l'unité gNB-CU du plan utilisateur est sécurisé sur la base de la sécurité NDS/IP. On utilise la sécurité NDS/IP pour protéger le réseau de raccordement qui connecte un nœud gNB à un réseau central, à moins que le réseau de raccordement soit doté d'une protection physique. Étant donné qu'une fonction UPF pourrait être déployée à la périphérie du réseau, on utilise également la sécurité NDS/IP pour protéger la communication entre la fonction UPF et la fonction SMF. Les services et fonctions de sécurité ci-après, qui sont liés à l'architecture de sécurité du réseau d'accès, sont présentés brièvement:

– Respect de la vie privée de l'abonné.
– Authentification.
– Hiérarchie des clés.
– Sécurité des données de signalisation NAS, de signalisation AS et d'utilisateur.
– Sécurité NDS/IP.
– Sécurité de l'accès non 3GPP.

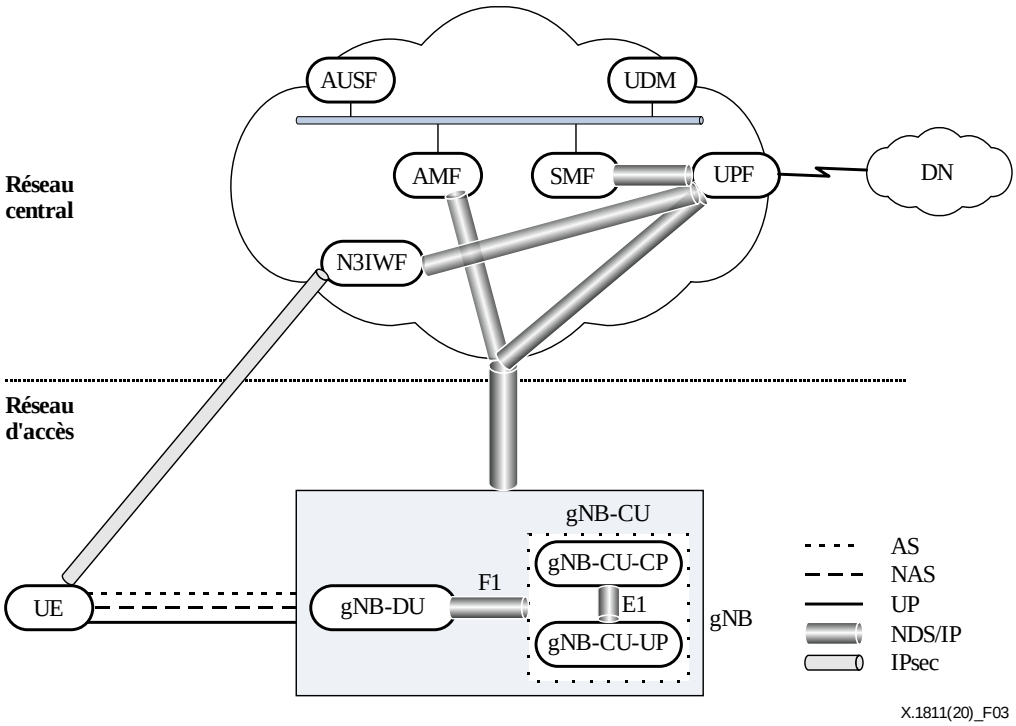

Figure 3 – Architecture de sécurité du réseau d'accès

7.2.1.1 Respect de la vie privée de l'abonné

Un équipement UE reçoit un identificateur SUPI dans le système IMT-2020, qui sera fourni dans le module USIM et dans le répertoire UDR de l'entité UDM. Un identificateur SUPI n'est jamais transmis non crypté dans l'interface hertzienne lorsqu'un module USIM IMT-2020 est déployé. Pour l'accès initial, l'équipement UE génère l'identificateur SUCI et le transmet à la fonction ARPF de l'entité UDM, comme indiqué dans la Figure 4. Lorsqu'elle reçoit un identificateur SUCI, la fonction SIDF située au niveau de l'entité UDM de la fonction ARPF procède à la suppression du masquage de l'identificateur SUPI à partir de l'identificateur SUCI. Sur la base de l'identificateur SUPI, la fonction ARPF de l'entité UDM choisit la méthode d'authentification conformément aux données d'abonnement.

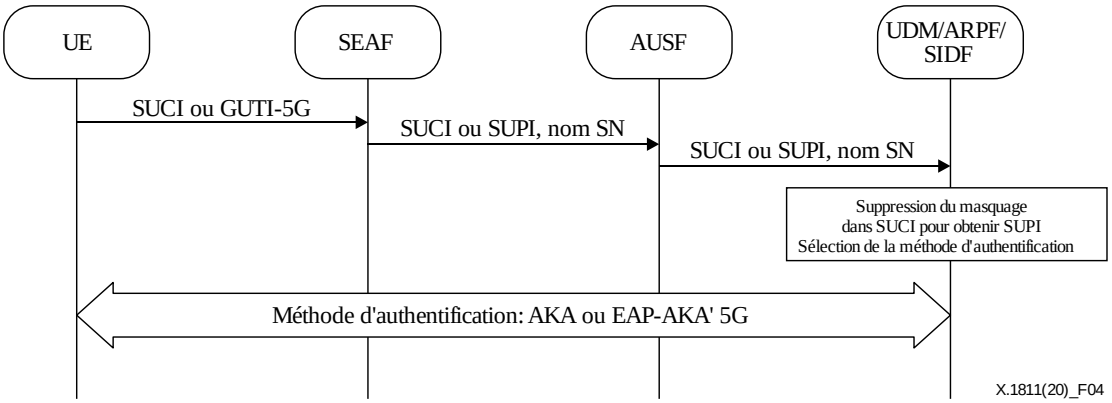

Figure 4 – Procédure d'authentification initiale et sélection de la méthode d'authentification (adaptée de la Figure 6.1.2-1 de [b-3GPP TS 33.501])

L'identificateur SUCI est composé d'une partie non cryptée et d'une partie cryptée. La partie non cryptée contient l'indicatif de pays du mobile et le code de réseau mobile, qui sont des informations relatives au réseau de rattachement permettant d'acheminer l'identificateur SUCI vers la fonction ARPF de l'entité UDM. La partie cryptée contient des informations sensibles relatives à l'abonnement, à savoir le numéro d'identification du mobile, qui est chiffré à l'aide du système ECIES. La clé publique du réseau de rattachement est mise en place de manière sécurisée dans le module USIM et dans la fonction SIDF, respectivement. Le principe du système ECIES est que l'équipement UE et le réseau appliquent leur propre clé privée et leur propre clé publique partenaire pour convenir de clés partagées en utilisant le mécanisme ECDH. Sur la base des clés partagées, la confidentialité des données et la protection de l'intégrité des données sont assurées moyennant l'utilisation d'algorithmes de chiffrement symétriques et d'algorithmes MAC, respectivement. Conformément aux profils spécifiés dans [b-3GPP TS 33.501], des mécanismes ECDH (X25519, primitive DH à cofacteur sur courbe elliptique) sont utilisés pour générer les clés partagées, le chiffrement AES-128 en mode compteur et l'algorithme HMAC-SHA-256 sont utilisés pour assurer la confidentialité des données et l'intégrité des données, respectivement.

Après le lancement de la procédure d'authentification, un identificateur temporaire unique à l'échelle mondiale IMT-2020 (IMT-2020-GUTI) est attribué de manière sécurisée à l'équipement UE afin de masquer l'identificateur SUPI pour le reste de la procédure d'authentification.

7.2.1.2 Authentification

Le système IMT-2020 applique deux types de protocole AKA pour l'authentification mutuelle entre l'équipement UE et le réseau, ainsi que la génération de clé de session K_{SEAF}, qui sont les protocoles 5G-AKA et d'authentification extensible – d'authentification et de concordance de clés (EAP-AKA') Le protocole EAP-AKA' peut être utilisé pour l'accès 3GPP et non 3GPP. Par rapport aux protocoles pour la 4G, les protocoles d'authentification IMT-2020 permettent un contrôle de rattachement

renforcé pour atténuer les risques de facturation frauduleuse de la part du réseau d'itinérance. Dans le cas du protocole EAP-AKA', la vérification de l'identité de l'équipement UE du côté du réseau est exécutée au niveau de la fonction AUSF du réseau de rattachement. Dans le cas du protocole 5G-AKA, bien que la vérification de l'identité de l'équipement UE du côté du réseau soit effectuée au niveau de la fonction SEAF du réseau d'itinérance, la fonction AUSF du réseau de rattachement vérifiera la confirmation de l'authentification pendant chaque procédure d'authentification.

Un ensemble d'algorithmes de génération de clés (*f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 et *f*5*) est utilisé lors de la procédure d'authentification pour générer le vecteur AV et la réponse authentification. Deux types d'ensembles d'algorithmes existent pour ce faire. L'un s'appelle l'ensemble d'algorithmes MILENAGE [b-ETSI 135 205], pour lequel le chiffrement AES-128 est recommandé comme base. L'autre s'appelle l'ensemble d'algorithmes TUAK [b-ETSI 135 231], pour lequel la fonction éponge Keccak [b-Bertoni] sert de base, avec une taille de clé d'entrée pouvant être de 128 bits ou 256 bits. Il est à noter que, dans la pratique, l'ensemble d'algorithmes MILENAGE est beaucoup plus déployé que l'ensemble TUAK.

7.2.1.3 Hiérarchie des clés

Sur la base de la clé racine K, l'équipement UE et le réseau effectuent l'authentification mutuelle et génèrent la clé de session K_{SEAF}, qui est l'ancre des clés (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) utilisées pour sécuriser la communication entre l'équipement UE et le réseau, comme le montre la Figure 5.

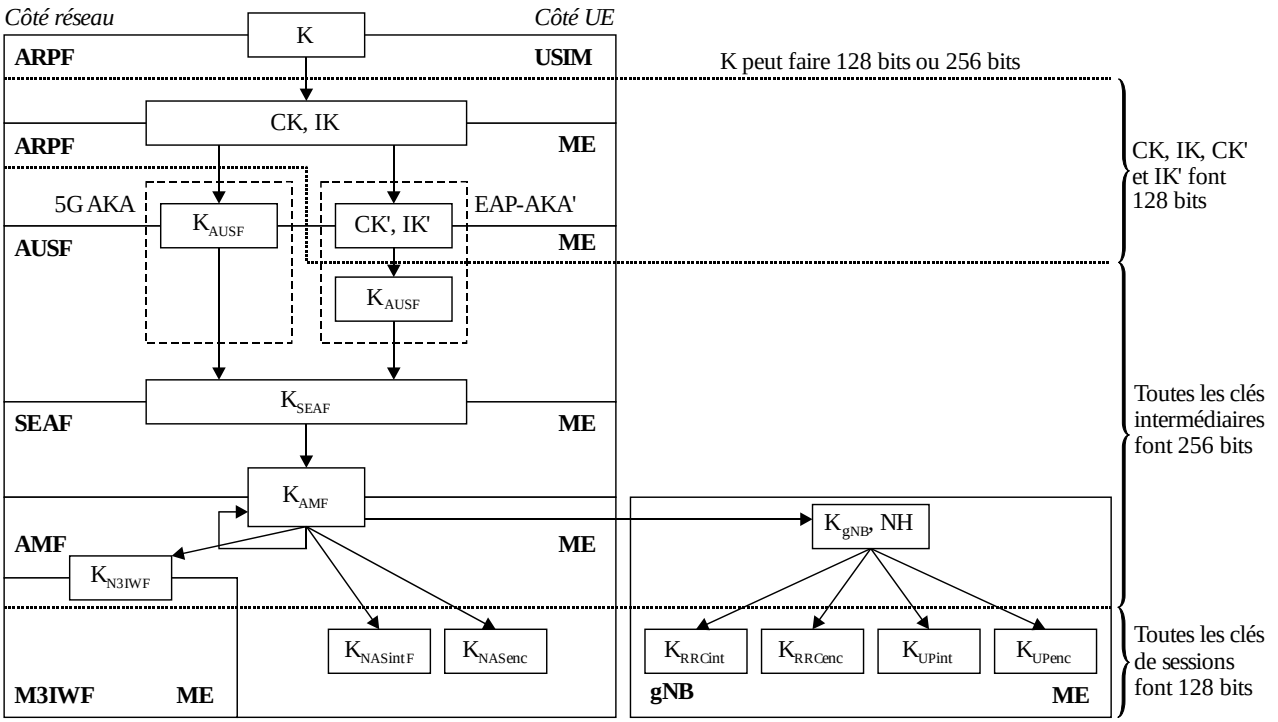

Figure 5 – Hiérarchie des clés (adaptée de la Figure 6.2.1-1 de [b-3GPP TS 33.501])

La longueur de la clé racine K peut être de 128 bits ou de 256 bits. Il convient de noter que la clé racine K dans les modules USIM classiques mesure toujours 128 bits, ce qui signifie que seules les clés racine de 128 bits sont fournies dans l'entité UDM pour le module USIM correspondant.

Les clés CK, IK, CK' et IK' sont les clés liées à la procédure d'authentification et ont une longueur de 128 bits. La génération des clés CK et IK repose sur l'ensemble d'algorithmes MILENAGE ou TUAK, tandis que la fonction GKDF définie dans [b-3GPP TS 33.220] est utilisée pour produire CK' et IK'.

Toutes les clés intermédiaires mesurent 256 bits et leur génération repose sur la fonction GKDF à l'exception de la clé K_{AUSF} dans le protocole EAP-AKA'. La fonction HMAC-HKDF décrite dans [b-IETF RFC 5869] est utilisée pour générer la clé K_{AUSF} dans le protocole EAP-AKA'.

Les clés (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) utilisées pour sécuriser la communication entre l'équipement UE et le réseau mesurent 128 bits et sont tronquées à partir du produit de 256 bits de la fonction GKDF.

7.2.1.4 Sécurité des données de signalisation NAS, de signalisation AS et d'utilisateur

Pour garantir la confidentialité des données de signalisation NAS, de signalisation AS et d'utilisateur, le système IMT-2020 doit prendre en charge le chiffrement 128-NEA1 (algorithme fondé sur 3G SNOW à 128 bits) et le chiffrement 128-NEA2 (algorithme fondé sur AES à 128 bits). De plus, le chiffrement 128-NEA3 (algorithme fondé sur ZUC à 128 bits) peut être pris en charge dans les systèmes IMT-2020.

Pour garantir l'intégrité des données de signalisation NAS, de signalisation AS et d'utilisateur, le système IMT-2020 doit prendre en charge le chiffrement 128-NIA1 (algorithme fondé sur 3G SNOW à 128 bits) et le chiffrement 128-NEA2 (algorithme fondé sur AES à 128 bits). De plus, le chiffrement 128-NEA3 (algorithme fondé sur ZUC à 128 bits) peut être pris en charge dans les systèmes IMT-2020.

7.2.1.5 Sécurité NDS/IP

L'interface entre le réseau d'accès et le réseau central (c'est-à-dire l'interface N2 entre le nœud gNB et la fonction AMF, l'interface N2 entre les fonctions N3IWF et AMF, l'interface N3 entre le nœud gNB et la fonction UPF, l'interface N3 entre les fonctions N3IWF et UPF), les interfaces entre les unités gNB-DU et gNB-CU (interface F1) et les interfaces entre les unités gNB-CU du plan de commande et gNB-CU du plan d'utilisateur (interface E1) sont protégées moyennant l'application de la sécurité NDS/IP ([b-3GPP TS 33.210], [b-3GPP TS 33.310]), qui spécifie le profil de sécurité utilisé dans les systèmes 3GPP pour les protocoles IPsec, IKEv2, TLS et DTLS [b-IETF RFC 6083].

Pour protéger l'intégrité et la confidentialité des données transmises via l'interface N2, l'interface E1 et l'interface F1, ainsi que pour prévenir les attaques par répétition, il est recommandé de mettre en œuvre l'authentification fondée sur des certificats IPsec ESP et IKEv2. En outre, le protocole DTLS doit être pris en charge.

Pour assurer l'intégrité, la confidentialité et la protection des réponses pour le trafic via l'interface N3, il est recommandé de mettre en œuvre l'authentification fondée sur des certificats IPsec ESP et IKEv2.

Pour ce qui est des algorithmes de chiffrement ESP, la norme AES-CBC et la norme AES-GCM avec une valeur ICV de 16 octets doivent être prises en charge, en plus du chiffrement AES-256. Pour ce qui est des algorithmes d'authentification ESP, la norme HMAC-SHA1-96 et la norme AES-GMAC avec chiffrement AES-128 doivent être prises en charge.

Pour ce qui est du protocole IKEv2, les algorithmes suivants doivent être pris en charge:

- Confidentialité: ENCR_AES_CBC avec une longueur de clé de 128 bits, AES-GCM avec une valeur ICV de 16 octets et une longueur de clé de 128 bits.
- Fonction pseudo-aléatoire: PRF_HMAC_SHA1, PRF_HMAC_SHA2_256.
- Intégrité: AUTH_HMAC_SHA256_128.
- Groupe DH 14 (MODP 2 048 bits),19 (groupe ECP aléatoire 256 bits).

Pour ce qui est du protocole IKEv2, pour garantir un niveau élevé de sécurité, les algorithmes suivants devraient être pris en charge:

- Confidentialité: AES-GCM avec une valeur ICV de 16 octets et une longueur de clé de 256 bits.

– Fonction pseudo-aléatoire: PRF_HMAC_SHA2_384.

– Groupe DH 20 (groupe ECP aléatoire 384 bits).

Le protocole DTLS 1.2 partage les mêmes suites de chiffrement que le protocole TLS 1.2, étant donné que le protocole DTLS 1.2, tel que spécifié dans [b-IETF RFC 6347], est fondé sur le protocole TLS 1.2. Les suites de chiffrement autorisées et obligatoires données dans TLS 1.2 [b-IETF RFC 5246] doivent être appliquées. En outre, les suites de chiffrement suivantes doivent obligatoirement être prises en charge et il est recommandé de les utiliser:

– TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 telle que définie dans [b-IETF RFC 5289].

– TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 telle que définie dans [b-IETF RFC 5288].

Pour garantir un niveau élevé de sécurité, la prise en charge des suites de chiffrement suivantes est recommandée:

– TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 telle que définie dans [b-IETF RFC 5289].

– TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 telle que définie dans [b-IETF RFC 5289].

Pour ce qui est des groupes DH, pour le mécanisme ECDHE, la courbe secp256r1 (P-256) telle que définie dans [b-IETF RFC 4492] doit être prise en charge, la courbe ecp384r1 (P-384) telle que définie dans [b-IETF RFC 4492] devrait être prise en charge. Pour le mode DHE, des groupes DH d'au moins 4 096 bits devraient être pris en charge; les groupes DH de moins de 2 048 bits ne doivent pas être pris en charge.

L'utilisation de l'authentification fondée sur des clés PSK est autorisée dans le protocole IK2v2, lors de la prise de contact avec le protocole TLS dans le contexte de la sécurité NDS/IP.

7.2.1.6 Sécurité de l'accès non 3GPP

On assure la sécurité de l'accès non 3GPP en établissant un tunnel IPsec entre l'équipement UE et la fonction N3IWF. Le protocole IKEv2 [b-IETF RFC 7296] est utilisé pour procéder à l'authentification mutuelle entre l'équipement UE et la fonction N3IWF sur la base de la clé K_{N3IWF}, afin d'établir une ou plusieurs associations de sécurité IPsec ESP [b-IETF RFC 4303] pour les tunnels IPsec.

La sécurité de la communication entre les fonctions N3IWF et AMF (interface N2), ainsi qu'entre les fonctions N3IWF et UPF (interface N3) est assurée moyennant l'utilisation de la sécurité NDS/IP.

7.2.2 Sécurité du réseau central

Il est prévu que le réseau central IMT-2020 soit construit sur la base d'un cadre NFV [b-ETSI GS NFV 002], dans lequel les fonctions NF sont découplées à partir de l'équipement dédié pour permettre un déploiement rapide des services et une meilleure efficacité d'exploitation. Comme on le voit dans la Figure 6, le cadre NFV peut être divisé en trois couches appelées infrastructure NFVI, fonctions VNF et services de réseau. Les fonctions VNF sont exécutées au-dessus de la couche NFVI commune pour fournir les services de réseau souhaités. La sécurité du réseau central est pour l'essentiel la sécurité de la couche VNF.

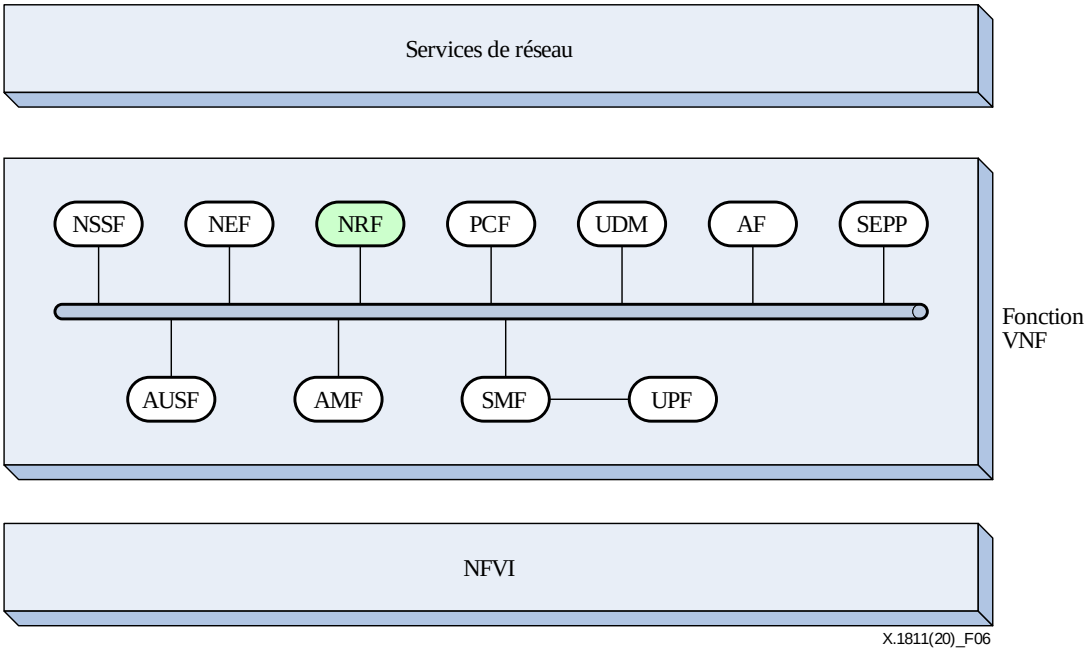

Figure 6 – Cadre du réseau central IMT-2020 fondé sur NFV (adaptée de la Figure 1 de [b-ETSI GS NFV 002])

Les fonctions VNF sont organisées en une architecture SBA, dans laquelle la fonction NRF joue un rôle clé dans le système. La fonction NRF décide si une fonction NF et autorisée à effectuer la découverte et l'enregistrement et délivre le jeton d'accès à la fonction NF. La sécurité des couches VNF peut être envisagée dans un réseau RMTP et entre réseaux RMTP, respectivement.

7.2.2.1 Dans un réseau RMTP

1) Authentification

Les fonctions NRF et NF doivent s'authentifier mutuellement lors du processus de découverte, d'enregistrement et de demande de jeton d'accès. Pour ce faire, il est possible d'utiliser la sécurité NDS/IP ou la sécurité physique. L'authentification entre les fonctions NF peut être effectuée de la même manière.

2) Autorisation

– Autorisation statique

Après que la fonction NF d'un consommateur de service et la fonction NF d'un producteur de service se sont authentifiées mutuellement, la fonction NF du producteur de service doit vérifier l'autorisation de la fonction NF du consommateur de service sur la base de la politique locale avant d'accorder l'accès à l'interface API du service.

– Autorisation fondée sur OAuth 2.0

Le contrôle d'accès pour les services de réseau fourni par les fonctions NF peut être mis en œuvre moyennant l'utilisation d'un cadre OAuth 2.0, spécifié dans [b-IETF RFC 6749]. Les jetons d'accès doivent être des jetons web JSON tels que décrits dans [b-IETF RFC 7519], sécurisés avec des signatures numériques ou des signatures numériques MAC fondées sur une signature JWS telle que décrite dans [b-IETF RFC 7515]. La fonction NRF joue le rôle de serveur d'autorisation OAuth 2.0. Le consommateur de service de la fonction NF et le producteur de service de la fonction NF correspondent respectivement au client OAuth 2.0 et au serveur de ressource OAuth 2.0. La communication entre les fonctions NF et la fonction NRF est protégée avec le protocole TLS, étant donné que des justificatifs d'identité sont transmis entre elles.

7.2.2.2 Entre réseaux RMTP

La sécurité entre réseaux RMTP est assurée par les proxy SEPP des deux réseaux via une interface N32, comme indiqué dans la Figure 7.

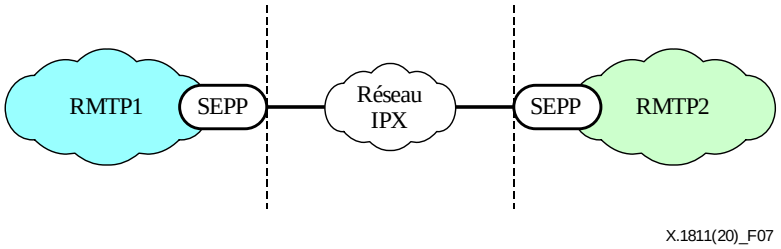

Figure 7 – Sécurité entre réseaux RMTP

L'interface N32 est composée d'une connexion N32-c et d'une connexion N32-f. La connexion N32-c est chargée de la gestion de l'interface N32, y compris d'une authentification AKA mutuelle entre les deux proxy SEPP au moyen du protocole TLS. La connexion N32-f est garante de l'envoi de messages protégés grâce au système JOSE entre les proxy SEPP.

Les proxy SEPP utilisent le chiffrement JWE (spécifié dans [b-IETF RFC 7516]) pour protéger les messages sur l'interface N32, où les clés convenues entre les deux proxy SEPP dans la connexion N32-c sont appliquées. Les fournisseurs IXP appliquent des signatures JWS, spécifiées dans [b-IETF RFC 7515], pour signer les modifications nécessaires pour leurs services de médiation.

Toutes les entités et fonctions qui prennent en charge le chiffrement JWE doivent utiliser les algorithmes [b-3GPP-TS 33.210] suivants: l'algorithme A128GCM avec paramètre "enc" (AES-GCM avec une clé de 128 bits) doit être pris en charge. L'algorithme A256GCM avec paramètre "enc" (utilisant une clé de 256 bits) devrait être pris en charge. L'algorithme "dir" avec paramètre "alg" (utilisation directe d'une clé symétrique partagée comme clé CEK) doit être pris en charge.

Toutes les entités et fonctions qui prennent en charge le chiffrement JWS doivent utiliser les algorithmes [b-3GPP-TS 33.210] suivants: l'algorithme ES256 avec paramètre "alg" (algorithme ECDSA utilisant la courbe P-256 ou l'algorithme SHA-256) doit être pris en charge.

7.3 Sécurité du plan de gestion

Le plan de gestion est composé d'un ensemble de gestionnaires (orchestrateur NFV, gestionnaire VNF, gestionnaire d'infrastructure virtualisée, contrôleur SDN, gestionnaire RAN). Cet ensemble de gestionnaires s'occupe de la gestion de la configuration, de la qualité de fonctionnement et des défaillances des objectifs correspondants via les interfaces. Toute modification, suppression, insertion ou répétition doit être empêchée pendant le transfert des données entre le gestionnaire et l'objectif de gestion [b-ETSI GS NFV-SEC 014]. Pour ce faire, le protocole TLS est appliqué à ces interfaces par défaut par les fabricants, comme indiqué dans la Figure 8.

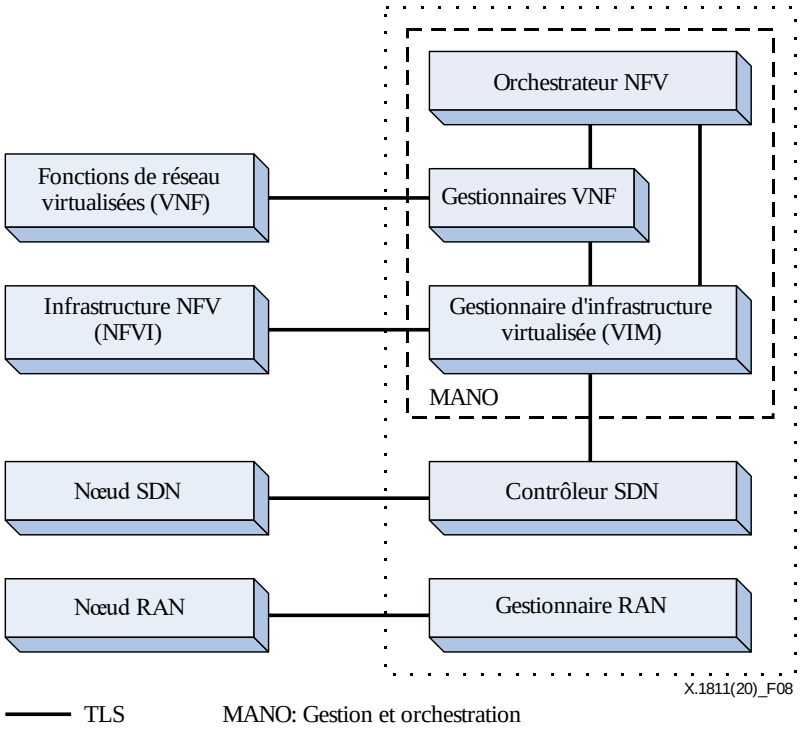

Figure 8 – Sécurité du plan de gestion

7.4 Récapitulatif des algorithmes de chiffrement utilisés dans les systèmes IMT-2020

Compte tenu de l'introduction à l'architecture de sécurité des systèmes IMT-2020 figurant dans les § 7.1 à 7.3, le Tableau 1 contient un récapitulatif des algorithmes de chiffrement utilisés dans les systèmes IMT-2020.

Tableau 1 –Algorithmes de chiffrement utilisés dans les systèmes IMT-2020

Type	Nom	Fonction	Scénario d'application
Algorithmes de chiffrement symétriques	128-NEA1	Chiffrement	Protection de la confidentialité entre l'équipement UE et la fonction AMF, ainsi qu'entre l'équipement UE et le nœud gNB
	128-NEA2		
	128-NEA3		
	128-NIA1	MAC	Protection de l'intégrité entre l'équipement UE et la fonction AMF, ainsi qu'entre l'équipement UE et le nœud gNB
	128-NIA2		
	128-NIA3		
	AES-128	Chiffrement	IPsec, TLS, DTLS, JWE, ECIES, NFVI
	AES-256	Chiffrement	IPsec, TLS, DTLS, JWE, NFVI
	Blowfish	Chiffrement	SDN
	3DES	Chiffrement	SDN
	SHA-256	Hachage	IPsec, TLS, DTLS, JWS, NFVI
	SHA-384	Hachage	IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-256	Calcul de clé/ MAC /Fonction pseudo–aléatoire	Hiérarchie des clés IPsec, TLS, DTLS, JWS, NFVI

Tableau 1 –Algorithmes de chiffrement utilisés dans les systèmes IMT-2020

Type	Nom	Fonction	Scénario d'application
	HMAC-SHA-384	Calcul de clé/MAC/ Fonction pseudo-aléatoire	IPsec, TLS, DTLS, JWS, NFVI
Algorithmes de chiffrement asymétriques	RSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	ECDSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	DH	Concordance de clés	IPsec, TLS, DTLS, NFVI
	ECDH	Concordance de clés	IPsec, TLS, DTLS, NFVI
NOTE 1 – L'algorithme SHA-1 est pas indiqué en raison de son faible niveau de sécurité. NOTE 2 – La longueur des clés pour les algorithmes de chiffrement asymétriques utilisés actuellement n'est pas indiquée étant donné que ces algorithmes peuvent être cassés quelle que soit la longueur de la clé si un ordinateur quantique à grande échelle est disponible. NOTE 3 – Pour des raisons de sécurité, la version du protocole TLS est la version 1.2 ou une version ultérieure.			

8 Évaluation de la sécurité des systèmes IMT-2020 dans le cadre de l'informatique quantique

Un ordinateur quantique est un dispositif qui exploite les phénomènes de la mécanique quantique (superposition et intrication) pour effectuer des calculs et manipuler de données. La sécurité des algorithmes de chiffrement les plus utilisés actuellement repose sur des problèmes mathématiques insolubles. En raison de l'attribut de parallélisme qui caractérise un ordinateur quantique, certains algorithmes quantiques peuvent résoudre des problèmes mathématiques difficiles plus efficacement que les algorithmes classiques, ce qui entraîne des menaces graves et crédibles sur le plan de la sécurité pour la cryptographique actuelle. L'Appendice III énumère les incidences de l'informatique quantique sur les algorithmes de chiffrement courants. Le paragraphe 8.1 présente les menaces que la disponibilité d'ordinateurs quantiques représente pour les algorithmes de chiffrement conventionnels. Les incidences des ordinateurs quantiques pour les systèmes IMT-2020 sont ensuite analysées.

8.1 Menaces pour les algorithmes de chiffrement conventionnels

8.1.1 Algorithmes de chiffrement asymétriques

L'algorithme de Shor permet de résoudre la factorisation d'un problème à entier élevé ou le problème du logarithme discret en temps polynomial [b-Shor 1999], ce qui détériore la sécurité des algorithmes asymétriques les plus utilisés actuellement. Cela signifie que la cryptographie à clé publique fondée sur RSA, dont la sécurité repose sur la factorisation d'un problème à entier élevé, et le protocole d'échange de clés DH, dont la sécurité repose sur le problème du logarithme discret, n'offriront aucune sécurité. Comme pour l'algorithme DH, la sécurité de l'algorithme DSA repose sur le problème du logarithme discret. Par conséquent, l'algorithme DSA est vulnérable aux attaques quantiques. L'algorithme ECC, dont la sécurité repose sur le problème ECDLP, a été très largement déployé parce qu'il est associé à une taille de clés bien plus petite que le système de clé publique fondé sur RSA. Or, il peut être cassé avec une variante de l'algorithme de Shor [b-Roetteler], ce qui implique que l'algorithme ECC, y compris les algorithmes ECDSA et ECDH, n'est pas sûr si des ordinateurs quantiques très puissants sont disponibles. Le Tableau 2 énumère les ressources quantiques nécessaires pour casser les algorithmes de chiffrement asymétriques qui sont couramment utilisés actuellement.

Tableau 2 – Ressources quantiques nécessaires pour casser les algorithmes de chiffrement asymétriques

Algorithmes	Taille de la clé publique (bits)	Niveau de sécurité comparable à celui de l'algorithme symétrique (bits)	Qubits logiques	Qubits physiques (voir Note 1)	Portes de Toffoli (voir Note 1)	Temps nécessaire pour casser des algorithmes (Voir Note 2)
RSA [b-Häner]	1 024	80	2 050	$7{,}38 \times 10^{6}$	$5{,}81 \times 10^{11}$	9,68 h
	2 048	112	4 098	$1{,}48 \times 10^{7}$	$5{,}2 \times 10^{12}$	3 jours 14 h
	4 096	128	8 194	$2{,}95 \times 10^{7}$	$5{,}59 \times 10^{13}$	31 jours 21 h
Fondé sur ECC [Roetteler]	256	128	2 330	$8{,}39 \times 10^{6}$	$1{,}26 \times 10^{11}$	2,1 h
	384	192	3 484	$1{,}25 \times 10^{7}$	$4{,}52 \times 10^{11}$	7,5 h
	521	256	4 719	$1{,}69 \times 10^{7}$	$1{,}14 \times 10^{12}$	19 h
NOTE 1 – Les ordinateurs quantiques ont besoin de ces bits quantiques physiques supplémentaires pour la correction des erreurs. Le nombre estimé de qubits physiques par qubit logique varie de 10 à 10 000. En l'espèce, nous prenons pour hypothèse un qubit logique pour 3 600 qubits physiques, voir [b-Fowler]. NOTE 2 – Nous supposons que le temps de fonctionnement d'une porte de Toffoli est de 60 ns, voir [b-Banchi].						

8.1.2 Algorithmes de chiffrement symétriques

L'algorithme de Grover permet une amélioration quadratique pour faire une recherche dans un ensemble de données non structuré sur des algorithmes classiques [b-Grover]. Il peut être exploité pour chercher la clé dans l'espace de clés d'un algorithme à clé symétrique. Dans le cas d'un algorithme à clé symétrique d'une longueur de n bits, il est possible de trouver la clé avec $O(2^{n/2})$ opérations quantiques sur une machine quantique contre $O(2^{n})$ opérations classiques sur un ordinateur conventionnel. Les ressources quantiques nécessaires pour chercher la clé d'un algorithme symétrique sont si importantes que la mise en œuvre de l'algorithme de Grover pour casser l'algorithme à clé symétrique sur un ordinateur quantique physique réel est discutable. Par exemple, une recherche de clé exhaustive pour un algorithme AES en utilisant l'algorithme de Grover nécessite les nombres suivants de portes de Toffoli et de Clifford: 2^{86} pour AES-128; 2^{118} pour AES-192; et 2^{151} pour AES-256, bien que le nombre de qubits logiques nécessaires soit compris entre 3 000 et 7 000 [b-Grassl].

L'algorithme de Grover coupe la clé effective en son milieu, c'est-à-dire qu'il réduit de moitié le niveau de sécurité d'un algorithme à clé symétrique. Ainsi, pour résister à l'informatique quantique, la longueur d'une clé pour un algorithme à clé symétrique doit être doublée.

8.1.3 Algorithmes de hachage

L'algorithme de Grover et sa variante ne permettent pas de trouver la collision d'une fonction de hachage plus rapidement que pour un algorithme classique [b-Bernstein 2009]. L'approche la plus efficace consisterait à utiliser une version parallèle de la méthode ρ de Pollard sur un groupe d'ordinateurs classiques [b-ETSI GR QSC 006]. Cela signifie que si les algorithmes de hachage utilisés actuellement sont sûrs, alors ils le seraient également en cas d'attaque informatique quantique à l'ère quantique. L'algorithme SHA-256 dont il est prouvé qu'il est sûr en informatique classique s'avère également capable de résister à une attaque de préimage quantique [b-Amy].

8.1.4 Fonctions de calcul de clé

Les fonctions KDF ont vocation à générer les clés utilisées pour garantir la confidentialité et la protection de l'intégrité, qui sont assurées en intégrant la clé partagée dans les fonctions de hachage.

Il existe deux types de fonctions KDF déployées dans les systèmes IMT-2020, à savoir la fonction GKDF définie dans [b-3GPP TS 33.220] et la fonction HKDF spécifiée dans [b-IETF RFC 5869].

La base des fonctions GKDF et HKDF est la fonction dispersée sur des clés HMAC-SHA-256. La sécurité du code HMAC dépend de la force du chiffrement de la fonction de hachage [b-IETF RFC 2104] utilisée. En conséquence, les fonctions KDF utilisées dans les systèmes IMT-2020 eux-mêmes ne sont pas notablement affectées par les progrès de l'informatique quantique.

Il est à noter que l'entropie du produit des fonctions KDF dépend de l'entropie de la clé d'entrée utilisée dans les fonctions KDF. Pour un produit entropique de 256 bits, une clé d'entrée de 256 bits est nécessaire lorsqu'on applique des fonctions KDF.

8.2 Prévision de calendrier pour le développement d'ordinateurs quantiques très puissants

Il est difficile de prédire à quelle échéance exacte des ordinateurs quantiques très puissants seront disponibles, car il n'y a pas de consensus sur cette question. [b-NISTIR 8105] estime qu'un ordinateur quantique d'un coût de 1 000 milliards USD pourrait casser un algorithme RSA de 2 048 bits en 2030. L'Institut européen des normes de télécommunication (ETSI) est arrivé à une conclusion similaire, à savoir que des ordinateurs très puissants pourraient être fabriqués en 2031 [b-ETSI GR QSC 004]. Ainsi, la sécurité des systèmes IMT-2020 risque d'être compromise, étant donné que ces systèmes seront exploités sur une durée allant de 10 à 20 ans. Par ailleurs, [b-NASEM] indique qu'il est très peu probable qu'un ordinateur quantique capable de casser un algorithme RSA de 2 048 bits puisse être fabriqué au cours des dix prochaines années. Cela ne signifie pas pour autant que les algorithmes de chiffrement résistant aux attaques quantiques ne devraient pas être étudiés et normalisés actuellement, puisque le délai nécessaire pour passer à un nouvel algorithme de sécurité est assez long et incertain [b-NASEM].

8.3 Incidences sur les systèmes IMT-2020

Comme nous l'avons vu dans le § 7, les protocole IPsec, TLS et DTLS ont été déployés à de nombreux endroits dans les réseaux IMT-2020. Il est nécessaire de donner tout d'abord un aperçu général pour évaluer les menaces que représentent les ordinateurs quantiques pour ces protocoles. Les incidences sur la sécurité des systèmes IMT-2020 seront ensuite évaluées selon la structure présentée dans le § 7.

8.3.1 Incidences sur les protocoles IPsec, TLS et DTLS

Bien que les protocoles IPsec, TLS et DTLS soient exécutés sur des couches différentes pour protéger la transmission des messages (IPsec résidant dans la couche réseau, TLS et DTLS résidant entre la couche réseau et la couche application), leur conception suit un principe analogue. Ils sont composés de deux parties: l'une est l'authentification et l'établissement de clés pour générer des clés de session, l'autre est la confidentialité et la protection de l'intégrité des messages moyennant l'utilisation d'algorithmes symétriques avec les clés de session.

Il existe deux méthodes pour procéder à l'authentification et à l'établissement de clés, fondées sur: 1) une clé symétrique pré-partagée; 2) une clé publique (un certificat est généralement utilisé).

Concernant la confidentialité et la protection de l'intégrité, les suites de chiffrement actuelles dans les protocoles IPsec, TLS et DTLS peuvent prendre en charge les algorithmes de chiffrement 128 bits et 256 bits.

En conséquence, nous pouvons évaluer si les protocoles IPsec, TLS et DTLS peuvent résister aux attaques informatiques quantiques en examinant les cas 1 à 4.

Cas 1: Authentification fondée sur une clé publique et algorithmes symétriques 128 bits ou 256 bits.

Dans ce cas, les clés de session peuvent être récupérées par l'auteur d'une attaque étant donné que les algorithmes asymétriques actuels indiqués dans les normes du Groupe d'étude sur l'ingénierie Internet (IETF) peuvent être cassés par des ordinateurs quantiques grâce à l'algorithme de Shor. Par

conséquent, quelle que soit la longueur de la clé utilisée par les algorithmes symétriques, la sécurité des messages transmis ne peut pas être garantie.

Cas 2: Authentification fondée sur une clé PSK de128 bits et algorithmes symétriques 128 bits.

Dans ce cas, à cause de l'algorithme de Grover, la longueur effective de la clé de sécurité est de 64 bits si un ordinateur quantique très puissant est disponible. Par conséquent, ces trois protocoles ne sont pas sûrs en cas d'attaque quantique.

Cas 3: Authentification fondée sur une clé PSK de 256 bits et algorithmes symétriques 128 bits.

Dans ce cas, bien qu'une clé PSK de 256 bits soit utilisée pour l'authentification et l'établissement de clé, seuls des algorithmes symétriques 128 bits sont appliqués pour la protection des messages. Par conséquent, le niveau de sécurité de ces trois protocoles est de 64 bits.

Cas 4: Authentification fondée sur une clé PSK de 256 bits et algorithmes symétriques 256 bits.

Dans ce cas, le niveau effectif de sécurité de ces trois protocoles est de 128 bits. Par conséquent, les attaques quantiques peuvent être déjouées avec l'utilisation de ce profil de chiffrement.

Seul le cas 4 est sûr en cas d'attaque quantique pour les profils de chiffrement actuels. Toutefois, l'authentification fondée sur une clé PSK ne convient que pour un petit groupe de communication car une clé PSK exige une configuration manuelle dans les dispositifs correspondants. Il est recommandé d'appliquer l'authentification fondée sur une clé publique lorsque le groupe de communication devient plus grand. Pour ce faire, il est recommandé d'introduire des algorithmes de chiffrement asymétriques résistant aux attaques quantiques dans les protocoles susmentionnés (c'est-à-dire IPsec, TLS et DTLS) pour l'authentification.

8.3.2 Incidences sur la couche infrastructure

Comme nous l'avons vu dans le § 7.1, le protocole TLS est utilisé pour protéger l'interface entre les applications et le contrôleur SDN, ainsi que l'interface entre le contrôleur SDN et les nœuds SDN. Le protocole IPsec peut être appliqué à l'interface entre le contrôleur SDN et les nœuds SDN. Comme le montre l'analyse présentée au § 8.3.1, ces deux interfaces sont vulnérables aux attaques quantiques, c'est-à-dire que l'auteur d'une attaque pourrait écouter, altérer et injecter des messages transmis via ces deux interfaces, sauf si les algorithmes indiqués dans le cas 4 sont déployés dans les protocoles TSL et IPsec.

La couche NFVI est vulnérable aux attaques quantiques car elle s'appuie sur des algorithmes de chiffrement asymétriques classiques pour mettre en œuvre certaines fonctions de sécurité, ce qui peut avoir de graves conséquences, comme l'accès illégal à la plate-forme pour installer des logiciels malveillants.

8.3.3 Incidences sur le réseau d'accès

8.3.3.1 Respect de la vie privée de l'abonné

On masque l'identificateur SUPI en le convertissant en identificateur SUCI avec le système ECIES comme présenté dans le § 7.2. Le mécanisme ECDH est utilisé pour convenir de la clé partagée entre l'équipement UE et le réseau dans le système ECIES. Il est possible de récupérer la clé partagée lors d'une attaque grâce à l'algorithme de Shor si des ordinateurs quantiques très puissants sont disponibles. Par conséquent, l'identificateur SUPI est révélé à l'auteur d'une attaque qui peut déchiffrer l'identificateur SUCI avec la clé partagée.

8.3.3.2 Authentification

Le protocole 5G AKA et le protocole EAP-AKA' procèdent à l'authentification mutuelle entre l'équipement UE et le réseau sur la base de la clé K à long terme, qui peut avoir une longueur de 128 bits ou de 256 bits. Dans le cas d'une clé K de 256 bits, jusqu'à présent, il n'y a eu aucune attaque visant les fonctions de hachage (c'est-à-dire l'ensemble d'algorithmes TUAK), qui sont la base

permettant de déduire les différents paramètres utilisés dans le protocole d'authentification, menée à l'aide d'un ordinateur classique. Par conséquent, ces deux protocoles d'authentification sont sûrs en cas d'attaque quantique, étant donné qu'il n'existe pas d'algorithme pour casser les fonctions de hachage qui soit plus efficace si l'on utilise un ordinateur quantique que si l'on utilise un ordinateur classique dans le contexte d'une clé K de 256 bits. S'agissant des clés K de 128 bits, dont le niveau effectif de sécurité est de 64 bits dans l'ère quantique, l'auteur d'une attaque peut récupérer la clé K à partir des messages interceptés liés aux deux protocoles d'authentification, par exemple les vecteurs AV, en effectuant 2^{64} opérations quantiques avec l'algorithme de Grover.

8.3.3.3 Hiérarchie des clés

La hiérarchie des clés est utilisée pour calculer des clés de 128 bits à partir de la clé K (racine) à long terme comme indiqué dans la Figure 5, afin de protéger la communication entre l'équipement UE et le réseau. Actuellement, la clé K de 128 bits est largement déployée, tandis que la clé K de 256 bits est rarement appliquée. Dans le cas d'une clé K de 128 bits, dont le niveau effectif de sécurité est de 64 bits dans l'ère quantique, le niveau de sécurité des clés calculées est de 64 bits. Par conséquent, l'auteur d'une attaque pourrait récupérer les clés à partir des messages interceptés chiffrés avec des clés de 128 bits.

8.3.3.4 Données de signalisation NAS, de signalisation AS et d'utilisateur

La confidentialité des données de signalisation NAS, de signalisation AS et d'utilisateur est protégée moyennant l'utilisation d'algorithmes symétriques avec des clés de 128 bits. Par conséquent, ces messages peuvent être déchiffrés par l'auteur d'une attaque avec un ordinateur quantique.

L'intégrité des données de signalisation NAS, de signalisation AS et d'utilisateur est protégée moyennant l'utilisation d'algorithmes MAC avec une clé de 128 bits. Le produit d'un algorithme MAC est tronqué en une étiquette d'une longueur de 32 bits qui est utilisée comme étiquette MAC. Il ne fait aucun doute que l'auteur d'une attaque peut construire un message après 231 tentatives si l'étiquette MAC a une longueur de 32 bits. Il est nécessaire d'étudier plus avant si la sécurité d'un système IMT-2020 est menacée si une étiquette MAC de 32 bits est tronquée à partir de l'étiquette originale de 64 bits ou de 128 bits.

8.3.3.5 Sécurité NDS/IP

Les protocoles TLS, DTLS et IPsec sont déployés pour protéger l'interface N2, l'interface N3, l'interface E1 et l'interface F1 comme indiqué au § 7.2.1, avec les mêmes incidences que pour la couche transport, à savoir que l'auteur d'une attaque peut écouter, altérer et injecter des messages transmis via ces interfaces, si les suites de chiffrement correspondant au cas 4 décrit au § 8.3.1 ne sont pas utilisées.

8.3.3.6 Sécurité de l'accès non 3GPP

L'accès non 3GPP est sécurisé grâce au protocole IPsec. Pour les raisons présentées au § 8.3.1, l'accès non 3GPP sécurisé ne peut être garanti, sauf si les suites de chiffrement correspondant au cas 4 décrit au § 8.3.1 sont utilisées.

8.3.4 Incidences sur le réseau central

8.3.4.1 Dans un réseau RMTP

1) Authentification

L'authentification entre fonctions FN ne sera pas affectée si son fonctionnement repose sur la sécurité physique. L'authentification peut être soumise aux mêmes menaces que celles indiquées au § 8.3.3 si elle se fait à l'aide de la sécurité NDS/IP.

2) Autorisation

L'autorisation statique ne sera pas affectée, étant donné qu'aucun algorithme de chiffrement n'est appliqué.

Dans le cas de l'autorisation fondée sur OAuth 2.0, deux scénarios permettent de garantir l'intégrité du jeton d'accès. L'adversaire peut falsifier un jeton d'accès si son intégrité est protégée à l'aide d'une signature. À l'inverse, un jeton d'accès ne peut pas être falsifié si un code MAC avec une clé de 256 bits est appliqué pour protéger son intégrité. Les justificatifs d'identité utilisés pour l'autorisation peuvent être divulgués étant donné qu'ils sont transmis via le protocole TLS entre les fonctions NF, à moins que le cas 4 décrit au § 8.3.1 soit appliqué.

8.3.4.2 Entre réseaux RMTP

L'auteur d'une attaque pourrait écouter, altérer et injecter des messages transmis via l'interface N32 entre des réseaux RMTP. En effet, la connexion N32-c s'appuie sur une authentification fondée sur des certificats dans le protocole TLS pour établir les clés de session et l'auteur d'une attaque pourrait obtenir ces clés en utilisant un ordinateur quantique.

8.3.5 Incidences sur le plan de gestion

Des modifications, suppressions, insertions ou répétitions pendant le transfert des données entre le gestionnaire et les objectifs de gestion sont possibles, étant donné que le protocole TLS associé à une authentification fondée sur des certificats est déployé dans le plan de gestion, ce qui représente une grave menace pour les systèmes IMT-2020, étant donné qu'il est possible pour l'auteur d'une attaque d'avoir accès au système de gestion du réseau IMT-2020.

9 Algorithmes de chiffrement résistant aux attaques quantiques

L'informatique quantique introduit un modèle informatique complètement nouveau, ce qui aura des incidences sur la sécurité des algorithmes à clé symétrique (par exemple, chiffrement par bloc) et les algorithmes à clé publique (par exemple RSA), même si la gravité de ses incidences sera différente pour chaque type d'algorithmes.

[b-Moses] montre, d'une part, que l'informatique quantique a pour effet de diviser par deux le nombre de bits de la force de la clé pour un algorithme à clé symétrique quel qu'il soit et, d'autre part, que les ordinateurs quantiques peuvent exécuter des algorithmes (par exemple celui de [b-Grover]) et trouver une clé de chiffrement symétrique de N bits en $2^{N/2}$ opérations. Par conséquent, si l'informatique quantique devient réalité, les algorithmes à clé symétrique peuvent être protégés en doublant simplement la longueur de la clé. Évidemment, cela aura des incidences sur les performances de l'algorithme à clé symétrique.

S'agissant des algorithmes à clé asymétrique, comme les algorithmes RSA, DSA, ECC et DH, on pense que les répercussions de l'informatique quantique seront très graves. Les ordinateurs quantiques peuvent exécuter des algorithmes (par exemple celui de [b-Shor 1997]) qui cassent tous les systèmes à clé publique les plus utilisés en très peu de temps. Par exemple, un algorithme quantique appelé l'algorithme de Shor peut récupérer une clé RSA en temps polynomial [b-Moses].

Les algorithmes de chiffrement résistant aux attaques quantiques devraient être sélectionnés au regard de critères d'évaluation (voir l'Appendice IV pour des exemples de critères d'évaluation définis par le NIST).

9.1 Algorithmes à clé symétrique résistant aux attaques quantiques

Il est largement admis que les cryptosystèmes symétriques de base, tels que le chiffrement par bloc ou les fonctions de hachage, sont des algorithmes résistant aux attaques quantiques [b-CSA] comme le montre l'Appendice III. [b-UIT-T X.1197] donne une liste d'exemples d'algorithmes et de longueur de clés capables de résister aux attaques quantiques. L'avènement de l'utilisation d'ordinateurs

quantiques dans le domaine du chiffrement exigera notamment d'allonger la longueur des clés symétriques, ce qui nécessitera de doubler la longueur des clés actuellement utilisées pour les IMT-2020, qui est de 128 bits. [b-CSA] montre que la longueur de clés de 256 bits actuellement recommandée est jugée sûre, même contre l'algorithme de Grover.

9.2 Algorithmes à clé asymétrique résistant aux attaques quantiques

Bien que les ordinateurs quantiques puissent exécuter des algorithmes qui cassent les systèmes à clé publique actuels (par exemple, RSA et ECC) en peu de temps comme indiqué dans l'Appendice III, de nombreuses catégories de systèmes de chiffrement autres que le chiffrement RSA et ECC sont sûrs face à une attaque menée par un ordinateur quantique; ils sont décrits aux § 9.2.1 à 9.2.5. Une liste des normes actuelles concernant les algorithmes asymétriques résistant aux attaques quantiques est donnée dans [b-UIT-T X.1197].

NOTE – La distribution de clés quantiques (QKD, *quantum key distribution*) est une méthode de mise en œuvre de la concordance de clés dont il est prouvé qu'elle est solide face à l'informatique quantique.

9.2.1 Algorithmes fondés sur les réseaux euclidiens

Les algorithmes fondés sur les réseaux euclidiens sont basés sur certains problèmes difficiles bien connus concernant le treillis pour construire des primitives cryptographiques résistant aux attaques quantiques. L'un de ces problèmes est celui du plus court vecteur (SVP), qui vise à trouver le plus court vecteur non égal à zéro dans un treillis donné, dont il est établi qu'il est un problème NP difficile selon des réductions aléatoires [b-Ajtai].

[b-CSA] montre que les algorithmes fondés sur des treillis peuvent assurer la signature numérique, le chiffrement par clé publique ou privée et la concordance de clés. Des algorithmes fondés sur les réseaux euclidiens sont donnés dans le § II.1.

9.2.2 Algorithmes fondés sur le hachage

Les algorithmes fondés sur le hachage s'appuient sur la sécurité de la fonction de hachage cryptographique sous-jacente.

[b-CSA] montre que des algorithmes fondés sur le hachage sont utilisés pour les signatures numériques construites à l'aide de fonctions de hachage. Des algorithmes fondés sur le hachage sont donnés dans le § II.2.

9.2.3 Algorithmes fondés sur des codes

Les algorithmes fondés sur des codes s'appuient sur des codes correcteurs d'erreurs, dans lesquels les systèmes de codage sont difficiles à décoder efficacement, même pour un ordinateur quantique. Par exemple, le cryptosystème de McEliece [b-McEliece] est basé sur le problème NP difficile visant à décoder un code linéaire général.

[b-CSA] montre que les algorithmes fondés sur des codes peuvent assurer la signature numérique, le chiffrement par clé publique ou privée et la concordance de clés. Des algorithmes fondés sur des codes sont donnés dans le § II.3.

9.2.4 Algorithmes multivariés

Les algorithmes multivariés se basent sur la difficulté qu'il y a à résoudre des systèmes d'équations polynomiales multivariées non linéaires dans des champs finis. Ce problème est connu pour être un problème NP difficile [b-Garey].

[b-CSA] montre que les algorithmes multivariés peuvent assurer la signature numérique et le chiffrement par clé publique ou privée. Des systèmes pratiques de signature fondée sur des algorithmes multivariés sont donnés dans le § II.4.

9.2.5 Algorithmes fondés sur l'isogénie supersingulière

Les algorithmes fondés sur l'isogénie supère singulière sont construits sur la base de la difficulté que représente la récupération d'une isogénie inconnue entre une paire de courbes elliptiques supersingulières dont on sait qu'elles sont isogènes.

Ils offrent une sécurité parfaite vers l'aval et sont utilisés comme une solution simple résistant à l'informatique quantique pour remplacer les méthodes DH et ECDH. L'algorithme SIDH est un exemple type [b-Jao].

10 Lignes directrices relatives à l'utilisation d'algorithmes de chiffrement résistant aux attaques quantiques dans les systèmes IMT-2020

On examine tout d'abord sur le plan général le traitement de l'augmentation importante de la longueur des messages lorsque des algorithmes asymétriques résistant aux attaques quantiques sont introduits dans les systèmes IMT-2020. L'utilisation d'algorithmes de chiffrement résistant aux attaques quantiques dans les protocoles IPsec, TLS et DTLS est ensuite prise en compte, étant donné qu'ils ont été déployés à plus d'un endroit dans les systèmes IMT-2020. Des lignes directrices sont ensuite indiquées pour appliquer des algorithmes de chiffrement résistant aux attaques quantiques dans le réseau d'accès IMT-2020 et dans le réseau central IMT-2020, respectivement.

10.1 Taille des messages

La taille des messages qui contiennent une clé publique, un cryptogramme ou une signature augmentera de manière significative, étant donné que la longueur des clés publiques, des cryptogrammes ou des signatures pour les algorithmes asymétriques résistants aux attaques quantiques est généralement bien plus grande qu'avec des algorithmes asymétriques classiques. Par exemple, la taille d'une clé publique pour les algorithmes asymétriques résistant aux attaques quantiques varie de 726 octets à environ 1 Mo comme indiqué dans le § II.5, alors que la taille d'une clé publique pour les algorithmes asymétriques classiques est généralement comprise entre 32 octets et 256 octets seulement. Le National Institute of Standards and Technology (NIST) prévoit de normaliser plus d'un algorithme asymétrique résistant aux attaques quantiques. Ainsi, on a tendance à penser qu'il faudra choisir d'utiliser des algorithmes asymétriques résistant aux attaques quantiques avec une clé publique, une signature ou un cryptogramme plus court dans les systèmes IMT-2020. De plus, les normes applicables aux systèmes IMT-2020 doivent déterminer la taille adéquate des messages pour prendre en charge la clé publique, le cryptogramme ou la signature lorsque des algorithmes asymétriques résistant aux attaques quantiques sont déployés.

10.2 Protocoles IPsec, TLS et DTLS

Si une clé PSK est appliquée pour l'authentification et la concordance de clés, il est recommandé que la taille de la clé PSK soit de 256 bits, et il est recommandé d'utiliser des algorithmes symétriques résistant aux attaques quantiques ayant une longueur de clés de 256 bits pour la confidentialité et la protection de l'intégrité des messages transmis sur le réseau. En cas d'utilisation de systèmes d'authentification fondée sur des certificats, il est recommandé d'intégrer des algorithmes asymétriques résistant aux attaques quantiques dans les protocoles d'authentification afin de permettre une authentification et une concordance de clés de session à l'épreuve des attaques quantiques, tandis que pour la confidentialité et la protection de l'intégrité des messages, il est recommandé de déployer des algorithmes symétriques résistant aux attaques quantiques ayant une longueur de clés de 256 bits. De cette manière, le réseau SDN, la sécurité NDS/IP et le plan de gestion ne sont pas vulnérables aux attaques quantiques.

L'IETF n'a pas commencé à travailler sur la manière d'ajouter des algorithmes résistant aux attaques quantiques dans les suites de chiffrements des protocoles IPsec, TLS et DTLS, de même que le NIST n'a pas achevé la sélection des algorithmes asymétriques résistants aux attaques quantiques candidats. On pense que les projets de normes du NIST pourraient être disponibles entre 2022 et 2024

[b-Moody]. Une fois que l'IETF aura spécifié les suites de chiffrements résistant aux attaques quantiques pour les protocoles IPsec, TLS et DTLS, la bande passante hertzienne étant une ressource rare et les capacités de calcul dans les dispositifs limitées, il est recommandé de déployer une suite de chiffrement avec des clés plus petites et une opération de chiffrement haut débit dans les systèmes IMT-2020.

10.3 Couche infrastructure

Il est recommandé d'utiliser un réseau SDN pour appliquer les suggestions indiquées dans le § 10.2 à l'utilisation des protocoles IPsec et TLS.

Il est recommandé de remplacer les algorithmes de chiffrement classiques déployés dans la couche NFVI par des algorithmes de chiffrement résistants aux attaques quantiques, y compris ceux des types symétriques et asymétriques.

10.4 Réseau d'accès IMT-2020

10.4.1 Respect de la vie privé de l'abonné

Le système ECIES est recommandé pour appliquer des algorithmes asymétriques résistant aux attaques quantiques de type DH pour générer la clé partagée, tels que l'encapsulation SIKE et NewHope, qui ont été retenus pour la deuxième phase de sélection des algorithmes candidats dans le cadre du travail de normalisation PQC du NIST (voir l'Appendice II). Il est recommandé de masquer l'identificateur SUCI grâce à l'algorithme symétrique résistant aux attaques quantiques avec une clé partagée de 256 bits.

10.4.2 Authentification

Étant donné que l'ensemble d'algorithmes MILENAGE ne prend en charge qu'une entrée avec clé de 128 bits, alors que l'algorithme TUAK peut prendre en charge des clés de 256 bits, il est recommandé d'utiliser l'ensemble d'algorithmes TUAK dans la procédure d'authentification pour générer le vecteur AV et la réponse d'authentification plutôt que l'ensemble MILENAGE.

10.4.3 Hiérarchie des clés

Pour générer la clé de session K_{SEAF} avec une entropie de 256 bits, la hiérarchie des clés doit faire les adaptations suivantes: 1) il est recommandé que la taille de la clé racine K soit de 256 bits; 2) il est recommandé de ne plus tronquer les produits de 256 bits de la fonction GKDF.

Dans la pratique, la longueur de la clé racine K est généralement de 128 bits, en raison de l'utilisation de cartes USIM d'ancienne génération ayant cette configuration dans les systèmes IMT-2020; les nouvelles cartes USIM utilisées pour les premiers systèmes IMT-2020 par de nombreux opérateurs continueront de stocker uniquement une clé racine de 128 bits, ce qui a notamment pour conséquence que l'entropie de la clé de session K_{SEAF} déduite de la clé K n'est que de 128 bits, ce qui ne permet pas de résister aux attaques quantiques.

Pour renforcer la sécurité de la clé de session en cours K_{SEAF} lorsque la carte USIM est dotée d'une longueur de clé racine de 128 bits, la génération de la clé de session en cours K_{SEAF} se base non seulement sur la clé de la première session K_{SEAF}' déterminée par la clé K à long terme, mais aussi sur au moins une des clés additionnelles. Les clés additionnelles pourraient être la clé de session initiale $K_{SEAF\_INITIAL}$ générée la première fois que l'équipement UE se connecte au réseau et/ou la clé de session K_{SEAF_PRV} utilisée lors de la session précédente. La clé de la première session et les clés additionnelles sont des clés symétriques, ce qui signifie que l'équipement UE et le réseau les partagent. De cette manière, l'entropie de la clé de session en cours K_{SAEF} sera d'au moins 256 bits, étant donné que l'entropie de la clé de la première session K_{SEAF}' est de 128 bits et que l'entropie des clés additionnelles (clé $K_{SEAF\_INITIAL}$ et/ou clé K_{SEAF_PRV}) est d'au moins 128 bits.

À titre de bonnes pratiques, de nouvelles cartes SIM peuvent, à titre d'option, être utilisées pour obtenir une entropie de 256 bits pour la clé de session K_{SEAF}. Il peut s'agir de cartes SIM, USIM ou eSIM ou d'autres facteurs et types de forme SIM non normalisés avec les adaptations correspondantes permettant:

a) de stocker une clé racine de 256 bits, pour servir le même objectif que la clé racine K dans les anciennes cartes (U)SIM;

b) de prendre en charge une accélération matérielle pour la fonction KDF et la boucle centrale de chiffrement symétrique (par exemple AES) nécessaires dans les nouvelles cartes SIM. Ce point est d'autant plus utile pour l'Internet des objets et dans les pays où les téléphones classiques représentent une part importante du nombre total de dispositifs cellulaires en utilisation, et pourraient toutefois être rendus compatibles avec un système IMT-2020 résistant aux attaques quantiques (si non rapides) grâce à la réutilisation des fréquences et la traduction de protocole.

10.4.4 Sécurité des données de signalisation NAS, de signalisation AS et d'utilisateur

Comme nous l'avons vu dans le § 7, des algorithmes à clé symétrique de 128 bits, comme les algorithmes AES-128, SNOW, 3G et ZUC-128 constituent la base pour la confidentialité et la protection de l'intégrité des données de signalisation NAS, de signalisation AS et d'utilisateur dans un réseau d'accès IMT-2020.

Pour résister aux attaques quantiques, il est recommandé de déployer des algorithmes à clé symétrique de 256 bits dans les systèmes IMT-2020. Un code MAC plus long offre davantage d'assurance contre les attaques consistant à deviner le code MAC du message. [b-NIST SP 800-38B] recommande l'utilisation d'un code MAC d'au moins 64 bits pour se défendre contre les attaques consistant à deviner le code. La longueur du code MAC dans un réseau d'accès IMT-2020 n'est que de 32 bits. Les incidences sont importantes pour le réseau IMT-2020 et le protocole si la longueur du code MAC passe de 32 bits à 64 bits. Il est nécessaire d'étudier plus avant si un réseau d'accès IMT-2020 est toujours en mesure de se défendre contre des attaques visant à deviner le code lorsque des algorithmes symétriques 256 bits résistants aux attaques quantiques sont appliqués pour générer un code MAC de 32 bits.

10.4.5 Sécurité de l'accès non 3GPP

Pour la stratégie permettant de résister aux attaques quantiques dans le cas de l'accès non 3GPP, voir le § 10.2, étant donné que la sécurité de l'accès non 3GPP s'appuie sur le protocole IPsec.

10.5 Réseau central IMT-2020

10.5.1 Dans un réseau RMTP

1) Authentification

Pour résister à une attaque quantique, il est recommandé d'appliquer pour l'authentification fondée sur la sécurité NDS/IP la stratégie décrite dans le § 10.2.

2) Autorisation

Il est recommandé de déployer des fonctions dispersées sur des clés résistant aux attaques quantiques, comme HMAC-SHA-256, ainsi que des algorithmes de signature résistant aux attaques quantiques, dans le protocole OAuth 2.0 pour garantir l'intégrité du jeton d'accès. Pour la stratégie permettant de passer à des suites de chiffrement résistant aux attaques quantiques dans le protocole TLS, voir le § 10.2.

10.5.2 Entre réseaux RMTP

Il est recommandé d'appliquer la méthode présentée dans le § 10.2 à la connexion N32-c pour empêcher l'auteur d'une attaque quantique de calculer les clés de session. Il est recommandé de déployer le chiffrement AES-GCM avec une clé de 256 bits dans une interface N32 pour garantir la confidentialité et l'intégrité de la communication entre réseaux RMTP.

Il est recommandé de déployer des algorithmes de signature résistant aux attaques quantiques à la place de l'algorithme ECDSA pour la signature JWS.

Appendice I

Aperçu général des systèmes IMT-2020

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

Le présent Appendice donne une description générale d'un système IMT-2020.

I.1 Architecture générale

Les systèmes IMT-2020 visent à fournir une gamme variée de services ayant des exigences de fonctionnement différentes. Selon les spécifications 3GPP, les services fournis dans les réseaux IMT-2020 peuvent être classés en trois catégories: 1) le large bande mobile évolué (eMBB), qui prend en charge des débits de données plus élevés et une plus grande mobilité de l'utilisateur que les technologies 4G/LTE; 2) l'Internet des objets massif (mIoT), qui prend en charge des communications massives de type machine; 3) les communications URLLC, qui prennent en charge des services essentiels pour la mission nécessitant une grande fiabilité et un faible temps de latence. Les systèmes IMT-2020 ont vocation à constituer une plate-forme souple permettant de mettre en place de nouveaux scénarios commerciaux et d'intégrer des secteurs verticaux, comme l'industrie automobile, l'industrie manufacturière, le secteur de l'énergie, la cybersanté et le divertissement. En outre, le déploiement et la maintenance seront plus faciles pour les systèmes IMT-2020 que pour les réseaux mobiles des générations précédentes. Pour répondre à ces exigences ambitieuses, des technologies innovantes ont été introduites dans les systèmes IMT-2020, par exemple le découpage du réseau, la virtualisation NFV, la technologie SDN, l'architecture SBA et la séparation unité centrale/unité répartie (CU/DU).

L'architecture générale des systèmes IMT-2020, illustrée dans la Figure I.1, peut être divisée comme suit: couche infrastructure, couche réseau, couche service et plan de gestion, en fonction des fonctionnalités.

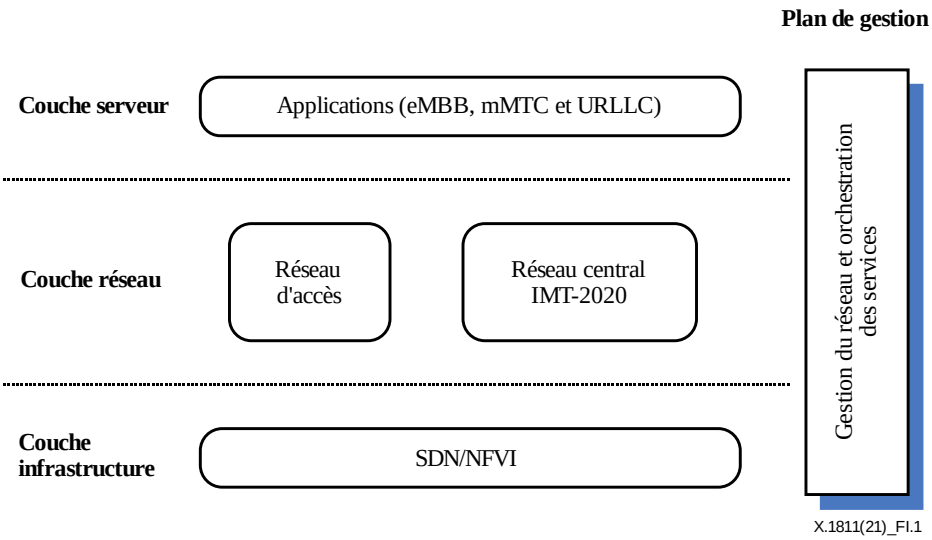

Figure I.1 – Architecture générale des systèmes IMT-2020

– La couche infrastructure comprend le réseau SDN et l'infrastructure NFVI. Le réseau SDN sert à transporter des paquets jusqu'à destination. Outre les anciennes technologies de transport (par exemple la commutation multiprotocole par étiquette (MPLS)), les systèmes IMT-2020 utilisent désormais la technologie SDN pour que le transport soit plus rapide et qu'il soit facile de s'adapter aux exigences des services. L'infrastructure NFVI constitue la base commune pour l'exécution des fonctions VNF.

– La couche réseau comprend le réseau d'accès et le réseau central. Le premier permet à l'équipement UE d'accéder à un réseau IMT-2020 où qu'il se trouve. Le second est conçu sur le modèle d'une architecture SBA dans un souci d'extensibilité et de simplicité. Il est composé d'un certain nombre de fonctions NF pour assurer la connectivité des données et le déploiement des services comme les fonctions AUSF, AMF et SMF.

– La couche service comprend Les applications qui s'exécutent au-dessus du système IMT-2020, par exemple les applications eMBB, les applications mMTC et les applications URLLC.

– Le plan de gestion est responsable de la gestion des réseaux et de l'orchestration des services.

I.2 Réseaux SDN

Le principe de base d'un réseau SDN est le suivant: le plan de données est dissocié du plan de commande, afin qu'il puisse prendre en charge la programmabilité dynamique des nœuds de réseau dans le cadre du processus de transmission des données. Le contrôleur SDN prend les décisions relatives au réseau et envoie les règles de transmission qui en découlent aux nœuds du réseau. Ce mécanisme de transmission simplifie la mise en place des nœuds de réseau et se traduit par une amélioration de la qualité de fonctionnement dans le plan de données. L'architecture SDN est décrite dans la Figure I.2.

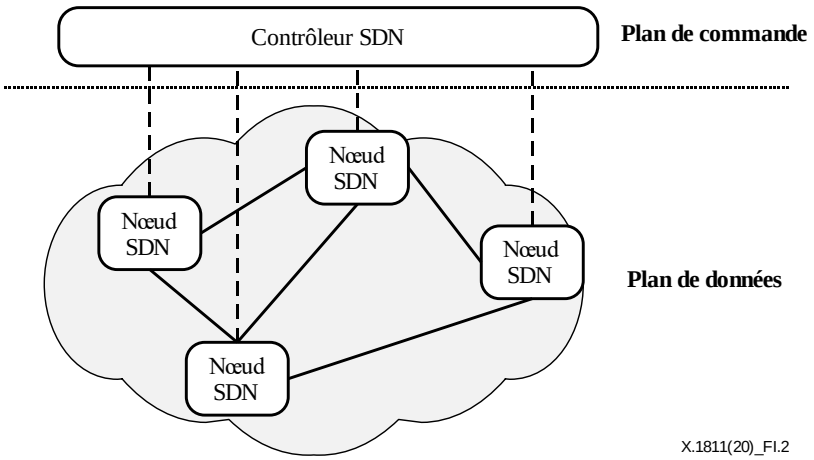

Figure I.2 – Architecture SDN

I.3 Réseau d'accès

L'équipement UE peut avoir accès à un réseau central IMT-2020 en utilisant un accès non 3GPP non sécurisé ou un accès 3GPP, comme le montre la Figure I.3. Le réseau d'accès assure des services liés à la transmission de données via l'interface radioélectrique.

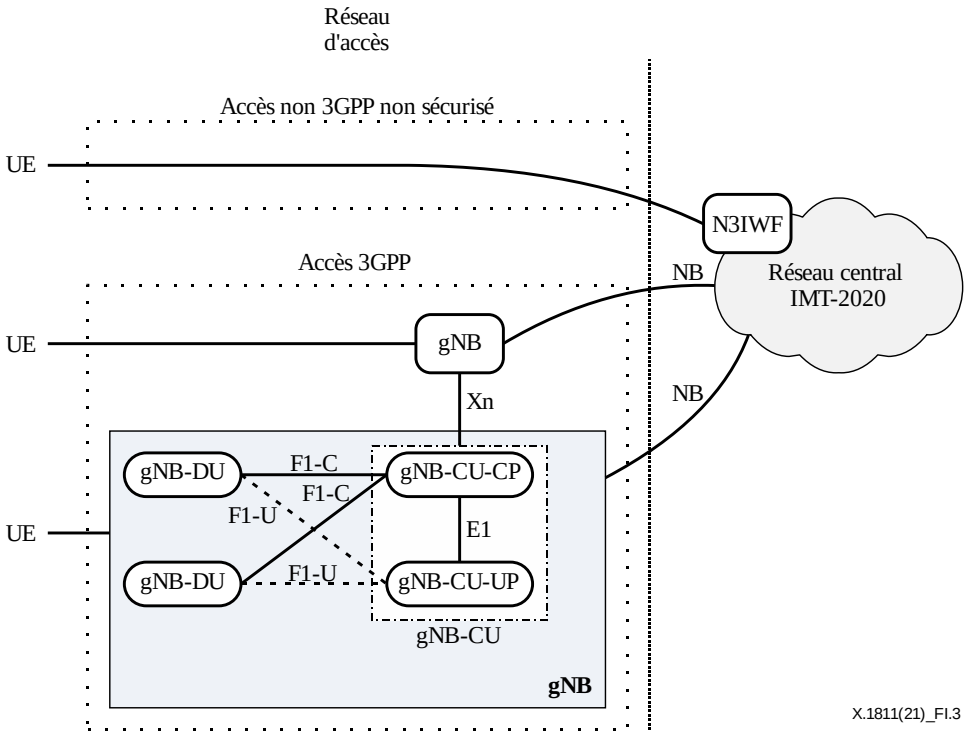

Figure I.3 – Réseau d'accès

– **Accès non 3GPP non sécurisé**

Un accès non 3GPP non sécurisé désigne une technologie d'accès qui n'est pas spécifiée par le 3GPP et à laquelle le réseau central IMT-2020 ne peut pas se fier, par exemple un accès WLAN. Dans ce cas, l'équipement UE se connecte au réseau central IMT-2020 via la fonction N3IWF.

– **Accès 3GPP**

L'accès 3GPP est une technologie d'accès spécifiée par le 3GPP, c'est-à-dire une technologie NG-RAN dans le contexte des IMT-2020. Un équipement UE peut accéder au réseau central IMT-2020 en utilisant une interface de prochaine génération à l'aide d'un nœud gNB simple sans séparation CU/DU. Une interface de prochaine génération est une interface logique prenant en charge l'échange d'informations CP et UP entre le nœud gNB et le réseau central IMT-2020. Afin d'assouplir le déploiement du réseau et de faire diminuer les coûts, il est possible de subdiviser un nœud gNB en un nœud gNB-DU et un nœud gNB-CU. Un nœud gNB-CU est un nœud logique qui met en œuvre les protocoles de la couche supérieure, notamment le protocole SDAP, le contrôle RRC et le protocole PDCP. Un nœud gNB-DU est un nœud logique qui assure des fonctions de la couche inférieure, notamment la commande RLC, la commande d'accès au support (MAC) et les fonctions de la couche physique.

Sur le modèle du concept des réseaux SDN, le nœud gNB-CU peut être encore subdivisé en un nœud gNB-CU-CP et un nœud gNB-CU-UP, ce qui permet de décomposer les fonctions de l'accès radioélectrique entre d'une part l'utilisateur, et d'autre part les entités du plan de commande. Une telle séparation du plan de commande et du plan d'utilisateur offre la souplesse nécessaire pour exploiter et gérer des réseaux complexes, en prenant en charge différentes topologies de réseau, ressources et nouvelles exigences pour les services.

Les unités gNB-CU et gNB-DU sont connectées à l'aide d'une interface logique F1, que l'on peut subdiviser en interface F1-C pour la connexion du nœud gNB-CU-CP et en interface F1-U pour la connexion du nœud gNB-CU-UP. Un nœud gNB-CU-CP communique avec un nœud gNB-CU-UP grâce à l'interface E1.

I.4 Réseau central

Le réseau central IMT-2020 est défini comme une architecture SBA, comme le montre la Figure I.4. Un certain nombre de fonctions NF ont été définies dans l'architecture SBA à différentes fins. Chaque fonction NF expose un ensemble de services appelé service NF et utilisé par d'autres fonctions NF autorisées. Les fonctions NF interrogent une fonction NRF pour se découvrir mutuellement et communiquer entre elles.

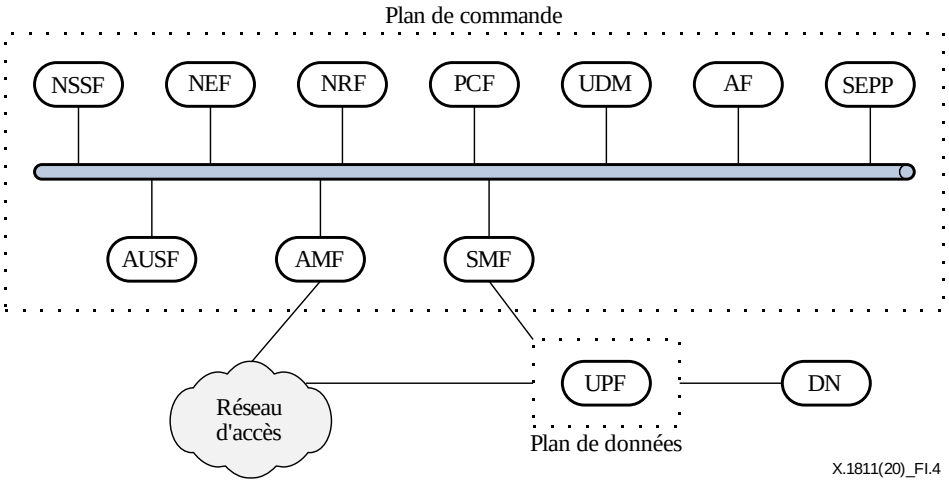

Figure I.4 – Réseau central IMT-2020

Le réseau central IMT-2020 peut être subdivisé en un plan de commande et un plan d'utilisateur.

– **Plan de commande**

  Ce plan assure des services de commande du réseau, notamment en ce qui concerne l'accès, la mobilité, la politique, l'exposition, l'interception licite et les commandes liées à la tarification. Les fonctions NF ci-après sont définies dans le plan de commande.

– **La fonction de sélection de tranche du réseau** (NSSF) sert à sélectionner l'ensemble d'instances de tranche de réseau utilisées pour l'équipement UE.

– **La fonction d'exposition du réseau** (NEF) prend en charge l'exposition des capacités et des événements. Les fonctions NF exposent les capacités et les événements à d'autres fonctions FN via la fonction NEF. Les capacités et événements exposés par des fonctions NF peuvent être exposés de manière sécurisée, par exemple à des tiers, à des fonctions d'application et des entités informatiques en périphérie.

– **La fonction de référentiel NF** (NRF) assure des fonctions d'enregistrement et d'identification de sorte que les fonctions NF peuvent se découvrir et communiquer entre elles via des interfaces API.

– **La fonction d'administration de la politique** (PCF) prend en charge un cadre politique unifié régissant le comportement du réseau.

– **La fonction de gestion de données unifiée** (UDM) stocke les données et les profils d'abonné. Elle est aussi utilisée pour générer les vecteurs AV pour l'authentification AKA 3GPP.

– **La fonction d'application** (AF) interagit avec le réseau central 3GPP pour fournir des services. Elle sert également à renseigner la fonction PCF sur le flux de paquets.

– **Le proxy de protection pour la sécurité en périphérie de réseau** (SEPP) est un proxy non transparent utilisé pour protéger les messages échangés via les interfaces CP entre réseaux RMTP et dissimuler la topologie du réseau à l'intérieur du réseau RMTP.

– **La fonction de serveur d'authentification** (AUSF) traite les demandes d'authentification pour l'accès 3GPP et l'accès non 3GPP.

– **La fonction de gestion de l'accès et de la mobilité** (AMF) assure l'authentification, l'autorisation et la gestion de la mobilité pour les équipements UE.

– **La fonction de gestion de session** (SMF) est utilisée pour la gestion des sessions, par exemple pour établir, modifier et libérer une session. Elle attribue également des adresses IP aux équipements UE.

– **Plan d'utilisateur**

  La fonction de plan d'utilisateur (UPF) est la seule fonction définie pour le plan d'utilisateur. Elle prend en charge diverses opérations et fonctionnalités liées aux paquets du plan d'utilisateur, par exemple le routage et la retransmission des paquets, la gestion du trafic, l'inspection des paquets et la duplication de paquets.

Le réseau central IMT-2020 est très différent des réseaux centraux des réseaux mobiles de génération précédente en ce qu'il a les caractéristiques suivantes:

– **L'architecture SBA**, dont les services fonctionnent avec une granularité plus fine que ceux des réseaux d'ancienne génération et font l'objet d'un couplage faible. De cette façon, il est possible de commercialiser de nouveaux services rapidement et de mettre à jour les systèmes avec plus de souplesse.

– **La séparation du plan de commande et du plan d'utilisateur**, qui permet de déployer la fonction UPF plus près de l'équipement UE, de sorte que ces exigences rigoureuses des services URLLC en matière de latence puissent être respectées. Cette séparation permet en outre de moduler les ressources de chacun des plans indépendamment.

– **La séparation des fonctions AMF et SMF**, qui permet de gérer l'accès et la mobilité de manière centralisée. La fonction SMF peut ainsi être située là où les services en ont besoin.

– **La fonction NFV**: le réseau central IMT-2020 part du principe que les fonctions NF sont mises en œuvre de manière virtuelle dans une optique d'optimisation de la gestion des ressources et de diminution des coûts. La séparation des éléments matériels et logiciels grâce à la fonction NFV rend le réseau plus flexible et plus simple car le poids des contraintes matérielles est réduit au minimum.

– **Le découpage du réseau**, qui vise à prendre en charge plusieurs types de services sur une même infrastructure de réseau physique. Il est ainsi possible d'adapter les réseaux de bout en bout pour répondre à différentes exigences. Chaque tranche de réseau peut contenir des fonctions NF différentes selon les exigences de service.

I.5 Plan de gestion

Le plan de gestion est responsable de la gestion des réseaux et de l'orchestration des services. Afin de gérer et de surveiller les réseaux, il se connecte au réseau d'accès, au réseau central et au réseau SDN au moyen d'un canal de communication individuel dédié, comme le montre la Figure I.5. La gestion des réseaux comprend au minimum les fonctionnalités suivantes: gestion des défaillances (FM), gestion de la qualité de fonctionnement (PM), gestion de la configuration (CM)et gestion des traces (TM). Outre ces fonctions de gestion du réseau, la gestion de la tranche de réseau nécessite également les fonctions suivantes: gestion du cycle de vie de la tranche, gestion des capacités de la tranche et découverte des ressources de réseau. L'orchestration des services consiste à appliquer des mécanismes souples de contrôle et de suivi des ressources à la fourniture, la gestion et la réoptimisation des services de réseau.

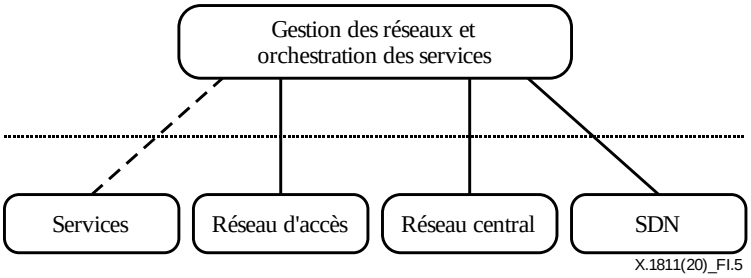

Figure I.5 – Architecture générale de gestion

Appendice II

Algorithmes asymétriques de chiffrement par clé résistant aux attaques quantiques

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

On trouvera dans le présent Appendice une liste d'algorithmes asymétriques de chiffrement par clé résistant aux attaques quantiques connus.

II.1 Algorithmes fondés sur les réseaux euclidiens

Les algorithmes basés sur les réseaux euclidiens comprennent notamment:

– l'anneau de polynôme tronqué de degré *N* (NTRU) [b-Hoffstein];
– l'apprentissage avec erreurs (LWE) [b-Regev];
– l'apprentissage en anneau avec erreurs (R-LWE) [b-Lyubashevsky];
– le système NewHope [b-Alkim].

II.2 Algorithmes fondés sur le hachage

Les algorithmes fondés sur le hachage comprennent notamment:

– le système de signature Merkle étendu (XMSS) [b-Buchmann];
– le modèle SPHINCS [b-Bernstein 2015];
– les signatures de Leighton-Micali fondées sur le hachage (LMS) [b-IRTF RFC 8554].

II.3 Algorithmes fondés sur des codes

Les algorithmes fondés sur des codes comprennent notamment:

– le modèle classique de McEliece [b-McEliece];
– le modèle de Niederreiter [b-Dinh].

II.4 Algorithmes multivariés

Les modèles de signatures pratiques fondés sur des algorithmes multivariés comprennent notamment:

– le modèle de Rainbow [b-Ding];
– le mélange non équilibré d'huile et de vinaigre (UOV) [b-Kipnis].

II.5 Normalisation de la cryptographie post-quantique par le NIST

Le 20 décembre 2016, le NIST a publié un appel à candidature concernant des algorithmes post-quantiques de chiffrement par clé publique. Lors de la première phase de sélection, le NIST a retenu 69 algorithmes candidats, dont 20 systèmes de signature numérique et 49 PKE ou KEM. Le 30 janvier 2019, au terme d'une deuxième phase de sélection, le NIST a retenu 26 algorithmes présentés dans le Tableau II.1, parmi lesquels 9 systèmes de signature numérique et 17 systèmes PKE et de création de clé [b-NISTIR 8240].

Tableau II.1 − Algorithmes retenus par le NIST au terme de la deuxième phase de la sélection

Type	Base du problème	Algorithme
Chiffrement/KEM	Fondé sur les réseaux euclidiens	Crystals-Kyber
		FrodoKEM
		LAC
		NewHope
		NTRU
		NTRU Prime
		Round 5
		Saber
		Three Bears
	Fondé sur des codes	Classic McEliece
		NTS-KEM
		BIKE
		HQC
		Rollo
		LEDAcrypt
		RQC
	Fondé sur l'isogénie	SIKE
Signature	Fondé sur les réseaux euclidiens	Crystals-Dilithium
		Falcon
		qTesla
	Multivarié	GeMSS
		LUOV
		MQDSS
		Rainbow
	Fondé sur le hachage	Sphincs+
		Picnic

Le NIST entend normaliser les algorithmes post-quantiques à clé publique destinés à être utilisés dans de nombreux protocoles différents, par exemple les protocoles TLS, SSH, IKE, IPsec et DNSSEC [b-NISTIR 8240].

Le NIST évalue les algorithmes retenus au terme de la deuxième phase de sélection tant sur le plan de la sécurité que sur le plan du fonctionnement. Le chiffrement NTRU a été inventé en 1996, et sa de sécurité est assez bien maîtrisée et étudiée de près depuis plusieurs décennies. De plus, ce type de chiffrement fait l'objet de la norme [b-IEEE Std 1363.1]. Le modèle classique de McEliece repose sur [b-McEliece], qui n'a jamais été cassé, et est considéré comme sûr dans un environnement quantique. En revanche, de nombreux autres systèmes ont été publiés il y a moins de 10 ans, de sorte que la communauté de la cryptographie doit encore en faire une cryptanalyse approfondie pour accroître la confiance dans leur sécurité. L'algorithme SIKE, qui est tiré de [b-Jao], repose sur le problème consistant à trouver des isogénies entre des courbes elliptiques supersingulières, lequel qui n'a pas été autant étudié que d'autres problèmes de sécurité associés à d'autres algorithmes candidates [b-NISTIR 8240].

Pour que la confidentialité vers l'avant soit totale, il faut que les clés des sessions antérieures ne soient pas dévoilées, même si la clé à long terme est exposée. Il s'agit d'une propriété de sécurité utile

souhaitée par des protocoles de sécurité très répandus tels que les protocoles IPsec et TLS. Parmi tous les algorithmes candidats, seuls les algorithmes SIKE et NewHope permettent d'assurer une confidentialité totale vers l'avant.

Le fonctionnement des algorithmes est évalué en fonction de la taille des clés publiques, des cryptogrammes et des signatures ainsi que de l'efficacité de calcul pour le chiffrement et le déchiffrement. Les clés publiques, les cryptogrammes et les signatures des algorithmes PQC sont en général beaucoup plus long que ceux des algorithmes à clé publique classiques. Selon [b-NIST PQC], la taille des clés publiques des algorithmes candidats va de 726 octets à plus de 1 Moctet. Si l'algorithme SIKE a la clé publique la plus petite, tandis que le système classique de McEliece et l'algorithme NTS-KEM ont une clé publique bien plus longue que d'autres systèmes, ils sont néanmoins capables de générer des cryptogrammes moins lourds que ceux produits par d'autres systèmes à une vitesse de chiffrement intéressante. Bien que sa clé publique soit la plus courte, l'algorithme SIKE semble être considérablement plus lent que bon nombre des autres algorithmes candidats. Il faut donc trouver un compromis entre l'efficacité d'utilisation de la bande passante et l'efficacité des calculs lorsque l'on choisit un algorithme PQC.

En 2020, le NIST compte soit choisir les finalistes en vue d'une phase finale de sélection, soit choisir un petit nombre d'algorithmes candidats qui seront normalisés [b-NISTIR 8240], ce qui signifie qu'il n'y aura pas qu'un seul algorithme PQC normalisé, mais plusieurs. Dans l'environnement mobile, l'efficacité revêt une importance critique étant donné que les ressources hertziennes des interfaces radioélectriques sont précieuses et les capacités de calcul des dispositifs limitées. Les algorithmes que l'on décidera de normaliser, qui seront associés à des clés publiques et des cryptogrammes de petite taille et offriront une vitesse de chiffrement concurrentielle, devraient être mis en place dans les systèmes IMT-2020.

Appendice III

Incidences de l'informatique quantique sur les algorithmes de chiffrement courants

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

On trouvera dans le présent Appendice une énumération des incidences de l'informatique quantique sur les algorithmes de chiffrement courants.

Le Tableau III.1 résume les incidences qu'ont les ordinateurs quantiques très puissants sur les algorithmes de chiffrement courants comme les algorithmes RSA et AES.

On ignore jusqu'où les avantages de l'informatique quantique peuvent aller et à quel point il reste du chemin à parcourir avant de pouvoir exploiter le modèle quantique en comparaison avec le modèle classique [b-NISTIR 8105].

Tableau III.1 – Incidences des ordinateurs quantiques sur les algorithmes de chiffrement couramment utilisés [b-NISTIR Quantum report]

Algorithme de chiffrement	Type	Utilisation	Incidence
AES	Symétrique	Chiffrement	Une clé de plus grande taille est nécessaire
SHA-2, SHA-3	Hachage	Fonction de hachage	Un résultat de plus grande taille est nécessaire
RSA	Clé publique	Signature, transport de clé	La sécurité n'est plus garantie
ECDSA, ECDH	Clé publique	Signature, échange de clé	La sécurité n'est plus garantie
DSA	Clé publique	Signature, échange de clé	La sécurité n'est plus garantie

Appendice IV

Critères d'évaluation du chiffrement résistant aux attaques quantiques

(Le présent Appendice ne fait pas partie intégrante de la Recommandation.)

On trouvera dans le présent Appendice les critères d'évaluation appliqués par le NIST pour sélectionner des méthodes de chiffrement à l'épreuve des attaques quantiques.

Les algorithmes de chiffrement présentés seront évalués selon trois critères: la sécurité, le coût et les caractéristiques de l'algorithme et de sa mise en œuvre [b-NIST-Sub].

IV.1 Sécurité

La sécurité garantie par un système de chiffrement est le critère d'évaluation le plus important. Les systèmes seront évalués à l'aune des facteurs suivants:

Applications du chiffrement par clé publique: des algorithmes post-quantiques seront normalisés pour les normes actuelles de chiffrement par clé publique applicables aux signatures numériques (FIPS 186) et à l'établissement de clés (SP 800-56A, SP 800-56B). Ils sont utilisés dans de nombreux protocoles Internet différents tels que les protocoles TLS, SSH, IKE, IPsec et DNSSEC. Les systèmes seront évalués en fonction du degré de sécurité qu'ils garantissent dans ces applications tout au long du processus d'évaluation. Les applications présentées seront évaluées en fonction de leur importance pratique si cela est nécessaire pour faire un choix parmi les algorithmes à normaliser.

Définition de la sécurité pour le chiffrement/l'établissement de clés: les algorithmes post-quantiques de chiffrement ou de d'établissement de clés devraient garantir une "sécurité sur le plan sémantique" vis-à-vis des attaques adaptatives à texte chiffré choisi. Cette propriété porte généralement le nom de sécurité *IND-CCA2* dans la littérature scientifique.

La définition de sécurité ci-dessus devrait être considérée comme définissant ce que le NIST estimera constituer une attaque. L'évaluation des systèmes de chiffrement et KEM présentés consistera à déterminer dans quelle mesure ils semblent présenter cette propriété lorsqu'ils sont utilisés conformément aux instructions de l'auteur. Celui-ci n'est pas dans l'obligation de fournir une preuve de sécurité, même si un tel élément sera pris en compte s'il est fourni.

Pour déterminer le degré de sécurité, on partira du principe que l'auteur de l'attaque a accès à la version déchiffrée d'au maximum 2^{64} cryptogrammes choisis; on pourra toutefois également envisager des attaques avec davantage de cryptogrammes.

Définition de la sécurité pour le chiffrement /la création de clés exclusivement éphémères: s'il est nécessaire que de nombreuses applications existantes garantissent la sécurité du cryptogramme choisi (par exemple les protocoles d'échange de clés explicitement éphémères permettant de placer les clés dans le cache), il est possible de mettre en œuvre un protocole d'échange de clés purement éphémères de sorte que la primitive de chiffrement ou du système KEM ait à assurer uniquement une sécurité passive.

Pour ces applications, les algorithmes post-quantiques de chiffrement/création de clés exclusivement éphémères devraient garantir la sécurité sémantique vis-à-vis des attaques à texte clair choisi. Cette propriété est couramment désignée sécurité *IND-CPA* dans la littérature scientifique.

L'évaluation des systèmes de chiffrement et KEM présentés consistera à déterminer dans quelle mesure ils semblent présenter cette propriété lorsqu'ils sont utilisés conformément aux instructions de l'auteur. Celui-ci n'est pas dans l'obligation de fournir une preuve de sécurité, même si un tel élément sera pris en compte s'il est fourni. Toute vulnérabilité concernant la sécurité induite par la réutilisation d'une clé devrait faire l'objet d'explications exhaustives.

Définition de la sécurité pour les signatures numériques: les algorithmes post-quantiques de signature numérique permettent de créer des signatures numériques intrinsèquement infalsifiables vis-à-vis d'une attaque adaptative à message choisi. Cette propriété porte généralement le nom de sécurité *EUF-CMA* dans la littérature scientifique.

L'évaluation des algorithmes de signature numérique présentés consistera à déterminer dans quelle mesure ils semblent présenter cette propriété lorsqu'ils sont utilisés conformément aux instructions de l'auteur.

Pour déterminer le degré de sécurité, on pourra partir du principe que l'auteur de l'attaque a accès aux signatures d'au maximum 2^{64} messages choisis.

Propriétés de sécurité additionnelles: si les définitions de la sécurité énumérées ci-dessus couvrent de nombreux scénarios d'attaque qui seront utilisés dans le cadre de l'évaluation des algorithmes présentés, d'autres propriétés sont souhaitables:

C'est notamment le cas de la confidentialité totale vers l'avant. Si l'utilisation de fonctionnalités de chiffrement et de signature habituelles permet de garantir cette propriété, le coût peut dans certains cas être prohibitif. On estime en particulier que les systèmes de chiffrement par clé publique dont l'algorithme d'établissement de clés est lent, comme l'algorithme RSA, ne sont généralement pas adaptés à la confidentialité totale vers l'avant. Dans ce cas, le coût et la sécurité pratique d'un algorithme sont étroitement liés.

La résistance aux attaques par voie latérale est un autre cas où sécurité et efficacité vont de pair. Les systèmes qu'il est possible de rendre résistants aux attaques par voie latérale à moindre coût sont préférables à ceux dont l'efficacité diminue fortement lorsque l'on tente de les rendre résistants aux attaques par voie latérale. Nous constatons en outre que les implémentations optimisées qui résistent aux attaques par voie latérale (par exemple les implémentations à temps constant) sont plus opérantes que les autres.

La troisième propriété souhaitable est la résistance aux attaques multi-clés. Dans l'idéal, l'auteur d'une attaque ne devrait pas obtenir un avantage s'il attaque plusieurs clés en même temps, qu'il ait l'intention de compromettre une seule paire de clés ou un plus grand nombre de clés.

La dernière propriété souhaitable, bien qu'elle soit encore mal définie, est la résistance aux mauvaises utilisations. Dans l'idéal, les systèmes ne devraient pas connaître de graves défaillances en cas d'erreurs de codage isolées, de dysfonctionnement du générateur de nombres aléatoires, de la réutilisation du nonce ou d'une paire de clés (dans le cas du chiffrement/de l'établissement de clés exclusivement éphémères), etc.

Autres facteurs à prendre en compte: étant donné que le chiffrement par clé publique est en général basé sur des structures mathématiques complexes, il est très important de bien comprendre la structure mathématique d'un système de chiffrement pour pouvoir avoir confiance dans son niveau de sécurité. Pour évaluer ce point, il faudra prendre en compte divers facteurs. Toutes choses étant par ailleurs égales, les systèmes simples sont généralement mieux compris que les systèmes complexes. De même, les systèmes fondés sur des principes pouvant être rattachés à un corpus d'études attestées sont généralement mieux compris que les systèmes entièrement nouveaux ou les systèmes conçus en apportant des corrections à d'anciens systèmes dont une cryptanalyse a révélé qu'ils étaient vulnérables.

Il sera tenu compte de la clarté des documents sur le système et de la qualité de l'analyse présentées par l'auteur. La clarté et l'exhaustivité de l'analyse aideront l'ensemble de la communauté à améliorer la qualité de cette analyse et à lui donner un caractère abouti. Tout argument ou preuve de sécurité fourni par l'auteur sera étudié. Si les preuves de sécurité reposent en général sur des hypothèses non vérifiées, elles permettent souvent d'écarter certaines classes d'attaque courantes ou de rattacher la sécurité d'un nouveau modèle à un problème de calcul plus ancien et mieux étudié.

IV.2 Coût

Le coût d'un système de chiffrement par clé publique peut être évalué à beaucoup de niveaux différents.

Taille de la clé publique, du cryptogramme et de la signature: les systèmes seront évalués en fonction de la taille des clés publiques, des cryptogrammes et des signatures qu'ils produisent. Il peut être important de tenir compte de tous ces facteurs dans le cas des applications à faible bande passante limitée ou des protocoles Internet dont la taille des paquets est limitée. L'importance de la taille de la clé publique peut dépendre de l'application; si une application peut placer les clés publiques dans le cache, ou éviter par un autre moyen de les communiquer fréquemment, la taille de ces clés importera sans doute moins. Au contraire, une application qui s'efforce d'assurer une confidentialité totale vers l'avant en communiquant une nouvelle clé publique au début de chaque session devrait tirer grandement parti des algorithmes qui utilisent des clés publiques relativement légères.

Efficacité des calculs pour les opérations relatives aux clés publiques et privées: les systèmes seront en outre évalués en fonction de l'efficacité des calculs pour les opérations relatives aux clés publiques (chiffrement, encapsulation et vérification de la signature) et aux clés privées (déchiffrement, désencapsulation et signature). Le coût des calculs pour ces opérations sera évalué sur les plans matériel et logiciel. Ce coût, tant pour les clés publiques que pour les clés privées, risque d'être élevé pour presque toutes les opérations, bien qu'une sensibilité à l'une ou à l'autre de ces opérations puisse être constatée dans certaines applications. Par exemple, les opérations de signature ou de déchiffrement peuvent être effectuées par un dispositif aux capacités de calcul limitées comme une carte intelligente; autre possibilité, un serveur traitant un gros volume de trafic devra peut-être consacrer une partie considérable de ses ressources de calcul pour vérifier les signatures des clients.

Efficacité des calculs pour l'établissement de clés: les systèmes seront en outre évalués en fonction de l'efficacité des calculs pour les opérations relatives à l'établissement de clés, le cas échéant. Le plus souvent, la durée nécessaire à l'établissement de clés est importante lorsqu'un algorithme de chiffrement par clé publique ou un système KEM est utilisé pour obtenir une confidentialité totale vers l'avant. Cependant, cette durée peut aussi être importante dans le cas des systèmes de signature numérique de certaines applications.

Échec de déchiffrement: il arrive parfois que des algorithmes de chiffrement par clé publique ou des systèmes KEM produisent un cryptogramme qu'il est impossible de déchiffrer/désencapsuler, même lorsqu'ils ont été mis en œuvre correctement. Pour la plupart des applications, il importe que ces échecs de déchiffrement soient rares, voire inexistants. Si un algorithme présente des échecs de déchiffrement/désencapsulation, les auteurs doivent communiquer le taux d'échec et une analyse des incidences que ces échecs sont susceptibles d'avoir en matière de sécurité. Si les applications peuvent garantir un taux d'échec de déchiffrement suffisamment bas en chiffrant plusieurs fois le même texte en clair et si les protocoles interactifs peuvent simplement redémarrer lorsque l'établissement de la clé échoue, ce type de solutions a un coût en termes de qualité de fonctionnement.

IV.3 Caractéristiques des algorithmes et des implémentations

Souplesse: pour autant qu'un bon niveau général de sécurité et de qualité de fonctionnement soit garanti, les systèmes offrant une plus grande souplesse répondront aux besoins d'un plus grand nombre d'utilisateurs que des modèles plus rigides, et ils leurs sont donc préférables.

Cette "souplesse" peut par exemple se manifester comme suit (sans que cette liste soit pour autant exhaustive):

1) Le système peut être modifié afin de fournir des fonctionnalités supplémentaires qui vont au-delà des exigences minimales applicables au chiffrement par clé publique, au mécanisme KEM (mécanisme d'encapsulation de la clé) ou à la signature numérique (par exemple les échanges asynchrones ou échanges de clés implicitement authentifiées, etc.).

2) Il est facile d'adapter les paramètres du système de façon à atteindre un certain nombre d'objectifs de sécurité et de qualité de fonctionnement.

3) Les algorithmes peuvent être mis en œuvre de manière sûre et efficace sur de nombreuses plates-formes différentes, y compris dans des environnements limités comme les cartes intelligentes.

4) Les implémentations des algorithmes peuvent être mises en parallèle afin d'améliorer la qualité de fonctionnement.

5) Le système peut être intégré dans des protocoles et applications existants en apportant le moins de modifications possibles.

Simplicité: le système sera évalué selon la simplicité de sa conception par rapport aux autres.

Adoption: les facteurs susceptibles de retarder ou d'encourager l'adoption généralisée d'un algorithme ou d'une implémentation seront pris en compte dans le processus d'évaluation. Il s'agit notamment des droits de propriété intellectuelle relatifs à un algorithme ou une implémentation, de la possibilité, pour les parties intéressées, d'acquérir une licence ainsi que des conditions d'octroi de cette licence. Les assurances fournies par le ou les auteur(s) et le ou les titulaire(s) de brevet seront prises en compte, une nette préférence étant accordée aux algorithmes présentés associés à un engagement d'octroi de licence sans contrepartie, selon des termes et conditions raisonnables, manifestement exempts de toute discrimination injuste.

Bibliographie

[b-UIT-T X.1196] Recommandation UIT-T X.1196 (2012), *Cadre du système de protection du service et de contenu téléchargeables dans l'environnement de la TVIP sur mobile.*

[b-ITU-T X.1197] Recommandation UIT-T X.1197 (2019), *Lignes directrices relatives aux critères de sélection d'algorithmes cryptographiques pour la protection de service et de contenu de TVIP*, Amendement 1.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités.*

[b-UIT-T Y.2014] Recommandation UIT-T Y.2014 (2008), *Fonctions de commande de rattachement au réseau dans les réseaux de prochaine génération.*

[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, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.

[b-ISO/CEI TR 22417] ISO/CEI TR 22417:2017, *Technologies de l'information – cas d'utilisation de l'Internet des objets (IoT)*.

[b-Ajtai] Ajtai, M. (1998). The shortest vector problem in L_2 is NP-hard for randomized reductions (résumé détaillé). In: Vitter, J. (éditeur). *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. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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. (éditeurs). *Selected areas in cryptography, SAC 2016*, St. Johns, Canada, 2016, p. 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. Disponible à l'adresse suivante [consulté le 02-02-2020]: 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*. Disponible à l'adresse suivante: 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. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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. (éditeurs). *Advances in Cryptology – EUROCRYPT 2015*, p. 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. (éditeur). *Post-quantum cryptography*, p. 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.* Disponible à l'adresse suivante [consulté le 03-02-2020]: 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. (éditeur). *Advances in cryptology—CRYPTO 2011*, p. 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. (éditeurs). *Applied Cryptography and Network Security, ACNS 2005*, p. 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. Disponible à l'adresse suivante [consulté le 02-02-2020]: 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 p.

[b-Grassl] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. In: Takagi T. (éditeur). *Post-quantum cryptography – PQCrypto 2016*, p. 29-43. *Lecture Notes in Computer Science*, volume 9606. Cham: Springer. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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*, p. 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. (éditeur). *Post-quantum cryptography*, p. 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. (éditeur). *Advances in Cryptology – EUROCRYPT '99*. p. 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, p. 114-116. Bibcode:1978DSNPR. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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 p. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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 p. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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 p. 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. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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)*. Disponible à l'adresse suivante [consulté le 14-02-2020]: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[b-NISTIR 8105] Rapport interne 8105 du National Institute of Standards and Technology (2016), *Report on post-quantum cryptography*. Gaithersberg, MA: National Institute of Standards and Technology. 15 p. DOI: 10.6028/NIST.IR.8105. Disponible à l'adresse suivante [consulté le 03-02-2020]: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[b-NISTIR 8240] Rapport interne 8240 du National Institute of Standards and Technology (2019), *Status report on the first round of the NIST post-quantum cryptography standardization process*. Gaithersberg, MA: National Institute of Standards and Technology. 27 p. DOI: 10.6028/NIST.IR.8240. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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. Disponible à l'adresse suivante [consulté le 14-02-2020]: 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 p. DOI: 10.6028/NIST.SP.800-38B. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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*. Disponible à l'adresse suivante [consulté le 02-02-2020]: 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', disponible à l'adresse suivante: https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/.

[b-QC2] Practical Quantum Computers, disponible à l'adresse suivante: 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*. p. 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. (éditeurs). *Advances in Cryptology – ASIACRYPT 2017*, p. 241-270. *Lecture Notes in Computer Science*, volume 10625. Cham: Springer. DOI: 10.1007/978-3-319-70697-9_9. Disponible à l'adresse suivante [consulté le 02-02-2020]: 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), p. 38-40. Disponible à l'adresse suivante [consulté le 03-02-2020]: 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), p. 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), p. 303-332. DOI: 10.1137/S0036144598347011.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021