Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1811

(04/2021)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las IMT-2020

Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2020

Recomendación UIT-T X.1811

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE LAS IMT-2020	**X.1800–X.1819**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1811

Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2020

Resumen

En la Recomendación UIT-T X.1811 se identifican las amenazas que plantea la informática cuántica a los sistemas de Telecomunicaciones Móviles Internacionales-2020 (IMT-2020) mediante la evaluación del grado de seguridad de los algoritmos criptográficos utilizados actualmente. En esta Recomendación se examinan brevemente los algoritmos de seguridad cuántica, incluidos los de tipo simétrico y asimétrico, y se proporcionan directrices para aplicar los algoritmos de seguridad cuántica en los sistemas IMT-2020.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1811	30-04-2021	17	11.1002/1000/14454

Palabras clave

Sistema 5G; algoritmo simétrico; sistema IMT-2020; ordenador cuántico; algoritmo de seguridad cuántica; algoritmo asimétrico.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

Índice

Página

Introducción

Los sistemas de Telecomunicaciones Móviles Internacionales-2020 (IMT-2020) prometen soportar una amplia gama de servicios con diversos requisitos de calidad de funcionamiento a fin de generar una sociedad totalmente conectada. Para alcanzar tan difícil objetivo se han creado tecnologías innovadoras en el contexto de los sistemas IMT-2020, como la segmentación de red, las redes definidas por *software*, la función de virtualización de red y la separación entre unidad central y unidad distribuida (CU/DU). Las medidas de seguridad son fundamentales para garantizar el funcionamiento normal de los sistemas IMT-2020. Además de algoritmos criptográficos simétricos, en los sistemas IMT-2020 se han implantado también algoritmos asimétricos.

Los grandes ordenadores cuánticos plantean problemas de seguridad para los algoritmos criptográficos simétricos y asimétricos actualmente utilizados, pues estos últimos no pueden ya garantizar la seguridad en la era de la informática cuántica. Además, los algoritmos criptográficos simétricos tienen que duplicar la longitud de sus claves para resistir los ataques informáticos cuánticos. Por este motivo resultaría muy conveniente utilizar en los sistemas IMT-2020 algoritmos criptográficos de seguridad cuántica.

En esta Recomendación se presentan brevemente los sistemas IMT-2020 y su arquitectura de seguridad. Se evalúan las amenazas que plantean los ordenadores cuánticos a los sistemas IMT-2020. También se hace un repaso de los algoritmos de seguridad cuántica, pero sin entrar en sus especificidades. Se incluirán en una Recomendación de alto nivel directrices de seguridad para adaptar los algoritmos de seguridad cuántica a los sistemas IMT-2020. El objetivo de esta Recomendación es ofrecer directrices para la utilización de algoritmos simétricos y asimétricos de seguridad cuántica en los sistemas IMT-2020 y para la armonización de los niveles de seguridad entre algoritmos simétricos y asimétricos de seguridad cuántica.

Recomendación UIT-T X.1811

Directrices de seguridad para la aplicación de algoritmos de seguridad cuántica en sistemas IMT-2020

1 Alcance

Esta Recomendación está compuesta por:

– una introducción a la arquitectura de seguridad de los sistemas de Telecomunicaciones Móviles Internacionales-2020 (IMT-2020);

– una evaluación de la seguridad de los sistemas IMT-2020 en presencia de ordenadores cuánticos comerciales;

– una especificación de la utilización de algoritmos de seguridad cuántica en sistemas IMT-2020.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se alienta a los usuarios de esta Recomendación a que investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[UIT-T X.1038] Recomendación UIT-T X.1038 (2016), *Requisitos de seguridad y arquitectura de referencia para las redes definidas por software*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 autentificación [b-UIT-T Y.2014]: Propiedad mediante la cual se establece la identidad correcta de una entidad o parte con la seguridad necesaria. La parte que se autentica puede ser un usuario, abonado, entorno doméstico o red de servicio.

3.1.2 protocolo de autentificación [b-UIT-T X.1254]: Secuencia definida de mensajes entre una entidad y un verificador que permite corroborar la identidad de la entidad.

3.1.3 autorización [b-ISO 7498-2]: Concesión de derechos, incluida la concesión de acceso en función de derechos de acceso.

3.1.4 disponibilidad [UIT-T X.800]: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.1.5 credencial [b-UIT-T X.1252]: Conjunto de datos presentados como prueba de una identidad y/o derechos declarados o aseverados.

3.1.6 confidencialidad [UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.7 integridad de los datos [UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.8 privacidad [UIT-T X.800]: Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada.

3.1.9 jerarquía de claves [b-UIT X.1196]: Estructura arborescente que representa la relación entre las distintas claves. En una jerarquía de claves, un nodo representa una clave utilizada para derivar las claves representadas por los nodos inferiores. Una clave sólo puede tener un nodo superior, pero puede tener múltiples nodos inferiores.

3.1.10 virtualización de la función de red (NFV, *network function virtualization*) [b-ISO/CEI TR 22417]: Tecnología que permite crear segmentos de red lógicamente aislados en redes físicas compartidas de manera que en las redes compartidas pueden coexistir simultáneamente conjuntos heterogéneos de múltiples redes virtuales.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas y acrónimos:

4G	Cuarta generación
AES	Norma de encriptación avanzada (*advanced encryption standard*)
AES-CBC	Norma de encriptación avanzada-encadenamiento de bloques cifrados (*advanced encryption standard-cipher blocker chaining*)
AES-GCM	Norma de encriptación avanzada-modo contador de Galois (*advanced encryption standard-galois counter mode*)
AES-GMAC	Norma de encriptación avanzada-código de autentificación de mensaje de Galois (*advanced encryption standard-galois message authentication code*)
AF	Función aplicación (*application function*)
AKA	Autentificación y acuerdo de clave (*authentication and key agreement*)
AMF	Función de gestión acceso y movilidad (*access and mobility management function*)
API	Interfaz de programación de aplicaciones (*application programming interface*)
ARPF	Función repositorio y procesamiento de credenciales de autentificación (*authentication credential repository and processing function*)
AS	Estrato de acceso (*access stratum*)
AUSF	Función servidor de autentificación (*authentication server function*)
AV	Vector de autentificación (*authentication vector*)
CEK	Clave de encriptación de contenido (*content encryption key*)
CM	Gestión de configuración (*configuration management*)
CP	Plano de control (*control plane*)
CU/DU	Unidad central/unidad distribuida (*central unit/distributed unit*)
DH	Diffie-Hellman
DHE	Efímero Diffie-Hellman (*Diffie-Hellman ephemeral*)

DNSSec	Extensión de seguridad del sistema de nombre de dominio (*domain name system security extensions*)
DSA	Algoritmos de firma digital (*digital signature algorithm*)
DTLS	Seguridad de la capa de transporte de datagramas (*datagram transport layer security*)
EAP	Protocolo de autentificación extensible (*extensible authentication protocol*)
ECC	Criptografía de curva elíptica (*elliptic-curve cryptography*)
ECDH	Diffie-Hellman de curva elíptica (*elliptic curve Diffie-Hellman*)
ECDHE	Efímero Diffie-Hellman de curva elíptica (*elliptic curve Diffie-Hellman ephemeral*)
ECDLP	Problema de logaritmo discreto de curva elíptica (*elliptic curve discrete-log problem*)
ECDSA	Algoritmo de firma digital de curva elíptica (*elliptic curve digital signature algorithm*)
ECIES	Esquema de encriptación integrado de curva elíptica (*elliptic curve integrated encryption scheme*)
ECP	Plano de corte extendido (*extended cutting plane*)
eMBB	Banda ancha móvil mejorada (*enhanced mobile broadband*)
ESP	Carga útil de seguridad de encapsulado (*encapsulating security payload*)
EU	Equipo de usuario
FM	Gestión de fallos (*fault management*)
GKDF	Función derivación de clave genérica (*generic key derivation function*)
gNB	Nodo B NR (*NR node B*)
GUTI	Identificador temporal exclusivo a nivel mundial (*globally unique temporary identifier*)
HKDF	Función derivación de claves por extracción y expansión basada en HMAC (*HMAC-based extract-and-expand key derivation function*)
HMAC	Código de autentificación de mensaje basado en número generador (*hash-based message authentication code*)
ICV	Valor de verificación de la integridad (*integrity check value*)
IKE	Intercambio de claves Internet (*Internet key exchange*)
IKEv2	Intercambio de claves Internet versión 2 (*Internet key exchange version 2*)
IMT-2020	Telecomunicaciones Móviles Internacionales-2020 (*International Mobile Telecommunications-2020*)
IPsec	Seguridad del protocolo Internet (*Internet protocol security*)
IP	Protocolo Internet (*Internet protocol*)
IPX	Central IP (*IP exchange*)
JOSE	Firma y encriptación de objetos Javascript (*javascript object signing and encryption*)
JSON	Notación de objeto JavaScript (*javascript object notation*)
JWE	Encriptación web JSON (*JSON web encryption*)

JWS	Firma web JSON (*JSON web signature*)
KDF	Función derivación de claves (*key derivation function*)
KEM	Mecanismo de encapsulación de claves (*key encapsulation mechanism*)
LTE	Evolución a largo plazo (*long-term evolution*)
LWE	Aprendizaje con errores (*learning with errors*)
MAC	Código de autentificación de mensaje (*message authentication code*)
mIoT	Internet de las cosas masiva (*massive Internet of things*)
mMTC	Comunicación tipo máquina masiva (*massive machine-type communication*)
MNO	Operador de red móvil (*mobile network operator*)
MODP	Exponencial modular (*modular exponential*)
MPLS	Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)
N3IWF	Función de interfuncionamiento no 3GPP (*non-3GPP interworking function*)
NAS	Estrato de no acceso (*non-access stratum*)
NDS	Seguridad del dominio de red (*network domain security*)
NEF	Función exposición de red (*network exposure function*)
NF	Función red (*network function*)
NFV	Virtualización de la función red (*network function virtualization*)
NFVI	Infraestructura de la virtualización de la función red (*network function virtualization infrastructure*)
NG-RAN	Red de acceso radioeléctrico de la próxima generación (*next generation-radio access network*)
NP	Tiempo polinómico no determinista (*non-deterministic polynomial time*)
NRF	Función repositorio NF (*NF repository function*)
NSSF	Función selección de segmento de red (*network slice selection function*)
NTRU	Anillo polinomial truncado de enésimo grado (*Nth degree truncated polynomial ring*)
PCF	Función control de política (*policy control function*)
PDCP	Protocolo de convergencia de datos en paquetes (*packet data convergence protocol*)
PKE	Encriptación de clave pública (*public-key encryption*)
PKI	Infraestructura de clave pública (*public-key infrastructure*)
PM	Gestión de calidad de funcionamiento (*performance management*)
PQC	Criptografía postcuántica (*post-quantum cryptography*)
PRF	Función pseudoaleatoria (*pseudo-random function*)
PSK	Clave precompartida (*pre-shared key*)
R-LWE	Aprendizaje con errores en anillo (*ring learning with errors*)
RLC	Control de enlace radioeléctrico (*radio link control*)
RPMT	Red pública móvil terrestre

RRC	Control de recursos radioeléctricos (*radio resource control*)
RSA	Rivest, Shamir y Adelman
SBA	Arquitectura basada en el servicio (*service-based architecture*)
SDAP	Protocolo de adaptación de datos de servicio (*service data adaptation protocol*)
SDN	Red definida por *software* (*software-defined network*)
SEAF	Función anclaje de seguridad (*security anchor function*)
SEPP	Intermediario de protección del perímetro de seguridad (*security edge protection proxy*)
SHA	Algoritmo de número generador seguro (*secure hash algorithm*)
SIDF	Función revelación del identificador de abono (*subscription identifier de-concealing function*)
SIDH	Isogenia Diffie-Hellman de extrema singularidad (*supersingular-isogeny Diffie-Hellman*)
SIKE	Encapsulación de claves de isogenia de extrema singularidad (*supersingular isogeny key encapsulation*)
SMF	Función gestión de sesión (*session management function*)
SSH	Intérprete de comandos seguro (*secure shell*)
SUCI	Identificador de abono oculto (*subscription concealed identifier*)
SUPI	Identificador de abono permanente (*subscription permanent identifier*)
SVP	Problema de vector más corto (*shortest vector problem*)
TLS	Seguridad de capa de transporte (*transport layer security*)
TM	Gestión de rastreo (*trace management*)
UDM	Gestión de datos unificados (*unified data management*)
UDR	Repositorio de datos de usuario (*user data repository*)
UOV	Aceite y vinagre desequilibrados (*unbalanced oil and vinegar*)
UP	Plano de usuario (*user plane*)
UPF	Función plano de usuario (*user plane function*)
URLLC	Comunicación ultrafiable y de baja latencia (*ultra-reliable and low-latency communication*)
USIM	Módulo universal de identidad de abonado (*universal subscriber identity module*)
VNF	Función red virtual (*virtual network function*)
WLAN	Red de área local inalámbrica (*wireless local area network*)
XMSS	Esquema de firma Merkle extendido (*extended Merkle signature scheme*)

5 Convenios

En la presente Recomendación:

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con la presente Recomendación.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para acreditar la conformidad.

La expresión "**se prohíbe**" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si la Recomendación pretende ser conforme.

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Generalidades

La tecnología de comunicación móvil IMT-2020 tiene la capacidad de colmar las necesidades comerciales ya presentes y que surgirán a partir de 2020. La arquitectura de seguridad es clave para el funcionamiento normal de una red IMT-2020. En la cuarta generación/evolución a largo plazo (4G/LTE) para proteger los datos de usuario y de señalización sólo se utilizan algoritmos simétricos. Además de esos algoritmos, los sistemas IMT-2020 introducen algoritmos asimétricos para proteger no sólo los identificadores de abonado, sino también la comunicación entre operadores de redes móviles (MNO, *mobile network operators*).

Hace poco (septiembre de 2020) IBM anunció un ordenador cuántico de 50 qubits [b-QC1], echando por tierra las previsiones de que los ordenadores cuánticos a gran escala no se comercializarían hasta dentro de 20 años. El nuevo informe [b-QC2] estima ahora plausible que estén disponibles en 10 años.

La seguridad de los algoritmos criptográficos de clave pública depende de la dificultad de los problemas de cálculo, como la factorización de enteros o el problema de logaritmo discreto en varios grupos. Se ha demostrado que los ordenadores cuánticos pueden solucionar eficazmente todos esos problemas [b-Shor 1997], anulando así los sistemas criptográficos de clave pública basados en esos supuestos. Por consiguiente, un ordenador cuántico con suficiente potencia podría poner en peligro muchos de los sistemas criptográficos modernos, como el intercambio de claves, la encriptación y la autentificación digital.

Los ordenadores cuánticos afectarán la solidez de la seguridad de los algoritmos simétricos y asimétricos en grado variable. La solidez de la criptografía simétrica se verá dividida entre dos, por ejemplo, una norma de encriptación avanzada (AES, *advanced encryption standard*) con claves de 128 bits que dan una solidez de 128 bits, se verá reducida a 64 bits, mientras que muchos de los algoritmos asimétricos más utilizados, como Rivest, Shamir y Adelman (RSA), algoritmo de firma digital (DSA, *digital signature algorithm*) y criptografía de curva elíptica (ECC, *elliptic-curve cryptography)*, no ofrecerán seguridad alguna.

El objetivo de los sistemas IMT-2020 es ofrecer una amplia gama de servicios con distintos requisitos de calidad de funcionamiento. Los servicios prestados a través de redes IMT-2020 pueden clasificarse en banda ancha móvil mejorada (eMBB, *enhanced mobile broadband*), Internet de las cosas masiva (mIoT, *massive Internet of things*) y comunicaciones ultrafiables y de baja latencia (URLLC, *ultra-reliable and low-latency communications*).

Los sistemas IMT-2020 introducen una serie de tecnologías innovadoras, como la segmentación de red, la virtualización de la función red (NFV, *network function virtualization*), las redes definidas por *software* (SDN, *software-defined network*) y la arquitectura basada en el servicio (SBA, *service-based architecture*). Estas tecnologías hacen de los sistemas IMT-2020 una plataforma flexible que permite nuevos usos comerciales e integra las industrias verticales. Por otra parte hacen que la arquitectura de seguridad de los sistemas IMT-2020 sea mucho más complicada que la de redes móviles de generaciones anteriores.

Hay un gran interés por estudiar cómo proteger las comunicaciones de sistemas IMT-2020 con algoritmos de seguridad cuántica porque es probable que los ordenadores cuánticos empiecen a comercializarse durante la vigencia de los sistemas IMT-2020. En la actualidad la longitud de clave de los algoritmos simétricos especificados para sistemas IMT-2020 es de 128 bits. El proyecto de asociación de tercera generación (3GPP, *3rd generation partnership project*) acaba de empezar un estudio sobre cómo aplicar algoritmos simétricos con claves de 256 bits de longitud a sistemas IMT-2020 [b-3GPP TR 33.841]. Sin embargo, hasta la fecha, ninguna organización ha estudiado cómo aplicar los algoritmos asimétricos de seguridad cuántica a los sistemas IMT-2020. Se ha de proceder a algún tipo de adaptación para utilizar algoritmos criptográficos de seguridad cuántica en los sistemas IMT-2020, pues sus claves son más largas que las utilizadas en la criptografía clásica. Además, es necesario estudiar la coexistencia de claves de distinta longitud en los sistemas IMT-2020, pues es imposible sustituir todos los algoritmos clásicos por otros de seguridad cuántica de un día para otro. La transición a la criptografía de seguridad cuántica de los sistemas IMT-2020 debe contemplarse con tiempo para que toda información que pueda verse en peligro más adelante a causa del criptoanálisis cuántico haya dejado de ser sensible.

En esta Recomendación se evalúan las amenazas que los ordenadores cuánticos plantean a los sistemas IMT-2020. Se hace un breve repaso de los algoritmos de seguridad cuántica, pero no se abordan en este documento sus especificidades. Las directrices de seguridad recomiendan, en términos generales, la adaptación de los algoritmos de seguridad cuántica a los sistemas IMT-2020. Esta Recomendación contiene unas directrices globales sobre la aplicación de algoritmos simétricos y asimétricos de seguridad cuántica en sistemas IMT-2020, además de la armonización de los niveles de seguridad entre algoritmos simétricos y asimétricos de seguridad cuántica.

7 Introducción a los componentes de seguridad de sistemas IMT-2020

En esta cláusula se da información básica sobre los componentes de seguridad de los sistemas IMT-2020 especificados por el UIT-T, 3GPP, ETSI, IETF, etc.

Un sistema de comunicación debe poder ofrecer algunos de los siguientes servicios de seguridad para garantizar la seguridad del sistema o de la transmisión de los datos [UIT-T X.800]: control de acceso (autorización); autentificación; privacidad; confidencialidad; integridad de los datos; no repudio, y disponibilidad.

La seguridad puede lograrse con mecanismos criptográficos o no criptográficos. Esta Recomendación se centra en los mecanismos criptográficos, pues estudia la aplicación de algoritmos criptográficos cuánticos en sistemas IMT-2020.

De acuerdo con la arquitectura de sistemas IMT-2020 presentada en el Apéndice I, puede decirse que la arquitectura de seguridad de los sistemas IMT-2020 se compone de tres capas: capa de infraestructura, capa de red y plano de gestión.

7.1 Seguridad de la capa de infraestructura

La capa de infraestructura es la base común que soporta la capa superior en los sistemas IMT-2020, que comprende la SDN y la capa de infraestructura de virtualización de la función red (NFVI, *network function virtualization infrastructure*).

7.1.1 Seguridad de la SDN

La tecnología SDN se utiliza para la entrega de datos en las IMT-2020 gracias a su gestión dinámica y flexible de los flujos de tráfico. La arquitectura de seguridad de la SDN se especifica en [UIT-T X.1038] y se ilustra esquemáticamente en la Figura 1.

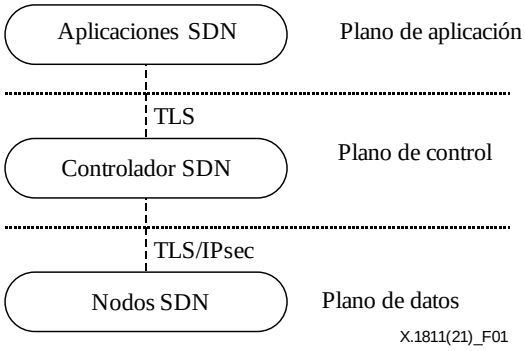

Figura 1 – Arquitectura de seguridad de la SDN

En [UIT-T X.1038] se formulan las siguientes recomendaciones en relación con los protocolos y algoritmos criptográficos.

Se recomienda el despliegue del protocolo de seguridad de la capa de transporte (TLS, *transport layer security*) [b-IETF RFC 5246] en la interfaz entre la aplicación SDN y el controlador SDN. De acuerdo con TLS, la aplicación SDN y el controlador SDN se autentifican mutuamente y acuerdan una clave de sesión. Además, quedan garantizadas la confidencialidad y la integridad de los datos en la interfaz de control de aplicación.

Se recomienda el despliegue del protocolo TLS [b-IETF RFC 5246] o el protocolo de seguridad del protocolo Internet (IPSec, *Internet protocol security*) ([b-IETF RFC 4301], [b-IETF RFC 4303], [b-IETF RFC 4835]) en la interfaz entre el controlador SDN y el nodo SDN. De acuerdo con TLS o IPsec, el nodo SDN y el controlador SDN se autentifican mutuamente y acuerdan una clave de sesión. Además, quedan garantizadas la confidencialidad y la integridad de los datos en la interfaz de nodo de control.

Los mecanismos de autentificación pueden basarse en una clave precompartida (PSK, *pre-shared key*) [b-IETF RFC 4279] [b-IETF RFC 4306] o en un certificado [b-IETF RFC 4306] y [b-IETF RFC 5246]. En la autentificación por certificado puede utilizarse el algoritmo RSA [b-ONF TR-511] o el algoritmo de firma digital. Para el acuerdo de una clave compartida entre dos entidades, en el contexto de TLS o IPSec pueden implementarse el protocolo de intercambio de claves Diffie-Hellman (DH) o el protocolo de intercambio de claves Diffie-Hellman de curva elíptica (ECDH, *elliptic curve Diffie-Hellman*).

Los algoritmos criptográficos utilizados para la encriptación de datos pueden ser AES [b-NIST FIPS 197], Blowfish [b-Schneier] o 3DES [b-NIST SP 800-67]. Los algoritmos criptográficos utilizados para los mecanismos de integridad de los datos pueden ser el código de autentificación de mensaje (MAC, *message authentication code*) [b-IETF RFC 2104], en código de autentificación de mensaje basado en número generador (HMAC, *hash-based message authentication code*) [b-IETF RFC 2104] o la firma digital [b-NIST FIPS 186-4].

7.1.2 Seguridad de la capa NFVI

La capa NFVI soporta la ejecución de las funciones de red virtual (VNF, *virtual network functions*), cuya estructura se muestra en la Figura 2.

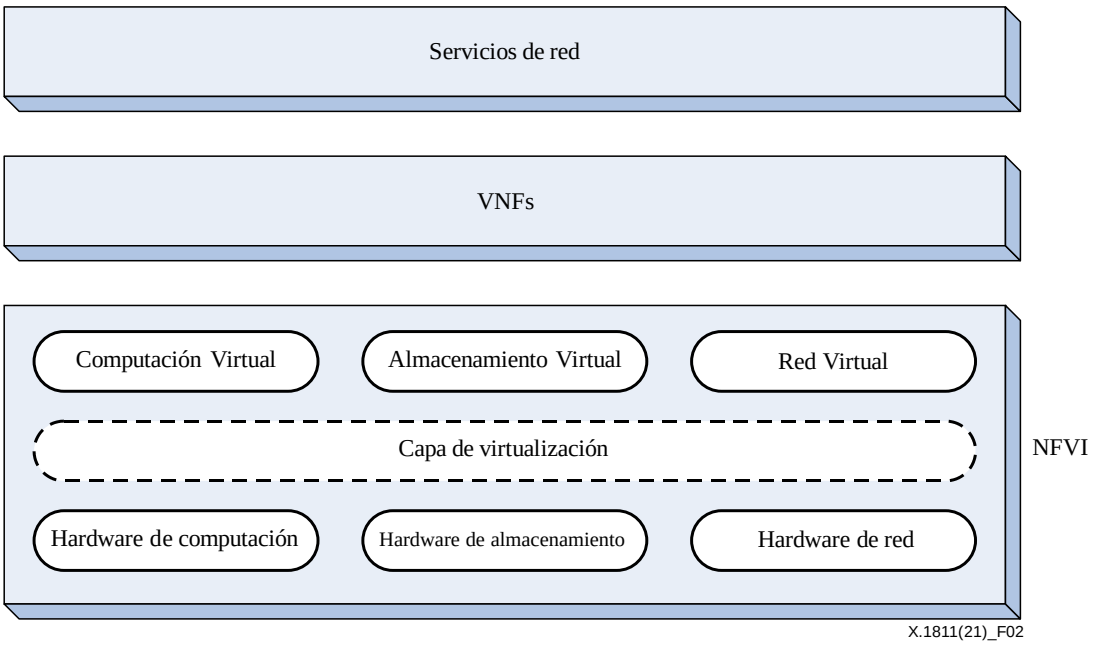

Figura 2 – Estructura de la NFVI (adaptada de la Figura 1 de [b-ETSI GS NFV 002])

De conformidad con [b-ETSI GS NFV-SEC 012], la NFVI deberá soportar las siguientes funciones de seguridad para garantizar la seguridad de las VNF que se ejecutan en ella: registro seguro; control de acceso y confinamiento a nivel de sistema operativo; controles físicos y alarmas; controles de autentificación; controles de acceso; seguridad de las comunicaciones; atestación; enclaves de ejecución por *hardware*; núcleo de confianza basado en *hardware*; almacenamiento autoencriptado; acceso directo a la memoria; módulos de seguridad de *hardware*, y protección y verificación de la integridad del *software*. Para ello, la NFVI implementará los siguientes algoritmos criptográficos [b-ETSI GS NFV-SEC 012]:

1) algoritmos de troceo: SHA-256, SHA-384, AES128-GMAC, HMAC-SHA128, HMAC-SHA256, HMAC-SHA384;
2) algoritmos de encriptación: AES-CBC-128, AES-GCM-128 (valor de verificación de la integridad (ICV, *integrity check value*) de 16 octetos), AES-CBC-256, AES-GCM-256 (ICV de 16 octetos);
3) firma: RSA 2048, RSA 3072, RSA 4096, ECDSA-256 (secp256r1), ECDSA-384 (secp384r1);
4) infraestructura de clave pública (PKI, *public-key infrastructure*): RSA 2048, RSA 3072, RSA 4096, id-ecPublicKey (secp256r1);
5) intercambio de claves: DH group 14 (exponencial modular (MODP, *modular exponential*) de 2 048 bits), DH group 19 (grupo de plano de corte extendido (ECP, *extended cutting plane*) aleatorio de 256 bits), DH group 20 (grupo ECP aleatorio de 384 bits), efímero Diffie-Hellman de curva elíptica (ECDHE, *elliptic curve Diffie-Hellman ephemeral*), secp256r1 (P-256), grupos de efímeros Diffie-Hellman (DHE, *Diffie-Hellman ephemeral*) de al menos 2 048 bits;
6) función pseudoaleatoria (PRF, *Pseudo-random function*): PRF-HMAC-SHA2-256, PRF-HMAC-SHA2-384.

7.2 Seguridad de la capa de red

7.2.1 Seguridad de la red de acceso

La seguridad de la red de acceso [b-3GPP TS 33.501] tiene por objetivo garantizar que el equipo de usuario (EU) autentificado puede acceder a la red IMT-2020 y que la comunicación entre el EU y la red IMT-2020 puede protegerse de la manera elegida en función de la política de seguridad del MNO.

La arquitectura de seguridad de la red de acceso IMT-2020 se ilustra en la Figura 3 y puede especificarse de la siguiente manera. El EU intenta acceder a la red con una identidad temporalmente asignada o una identidad permanente oculta antes de invocar el protocolo de autentificación y acuerdo de clave (AKA, *authentication and key agreement*). El EU y la red se autentifican mutuamente y acuerdan una clave de sesión ejecutando el protocolo AKA. El EU y la red derivan una serie de claves basadas en la clave de sesión. Sobre la base de esas claves, es obligatorio el intercambio de mensajes de señalización de integridad y protección de respuesta del estrato de no acceso (NAS, *non-access stratum*) entre el EU y la función de gestión acceso y movilidad (AMF, *mobility management function*), mientras que la protección de la confidencialidad es optativa; es obligatorio el intercambio de mensajes de señalización de integridad y protección de respuesta del estrato de acceso (AS, *access stratum*) entre el EU y el nodo B NR (gNB), mientras que la protección de su confidencialidad es optativa. La protección de la confidencialidad y la integridad de los datos de usuario en el plano de usuario (UP, *user plane*) entre el EU y el gNB es optativa. La comunicación entre el EU y la función de interfuncionamiento no 3GPP (N3IWF, *non-3GPP interworking function*) se protege utilizando un túnel IPsec cuando el acceso es no 3GPP. Dado que la gNB-DU y la gNB-CU pueden desplegarse en emplazamientos distintos, la interfaz F1 entre ellas se protege aplicando la seguridad del dominio de red/protocolo Internet (NDS/IP, *network domain security/Internet protocol*). Del mismo modo, la interfaz E1 entre un gNB-CU-CP y un gNB-CU-UP se asegura con NDS/IP. La red de retroceso que conecta un gNB con una red núcleo se protege mediante NDS/IP, a menos que la red de retroceso disponga de protección física. Dado que es posible desplegar una función plano de usuario (UPF, *user plane function*) en el borde de la red, la comunicación entre la UPF y la función gestión de sesión (SMF, *session management function*) también se asegura con NDS/IP. En relación con la arquitectura de seguridad de la red de acceso, se comentan brevemente los servicios o funciones de seguridad siguientes:

– privacidad del abonado;
– autentificación;
– jerarquía de claves;
– seguridad de la señalización NAS, la señalización AS y los datos de usuario;
– NDS/IP;
– seguridad del acceso no 3GPP

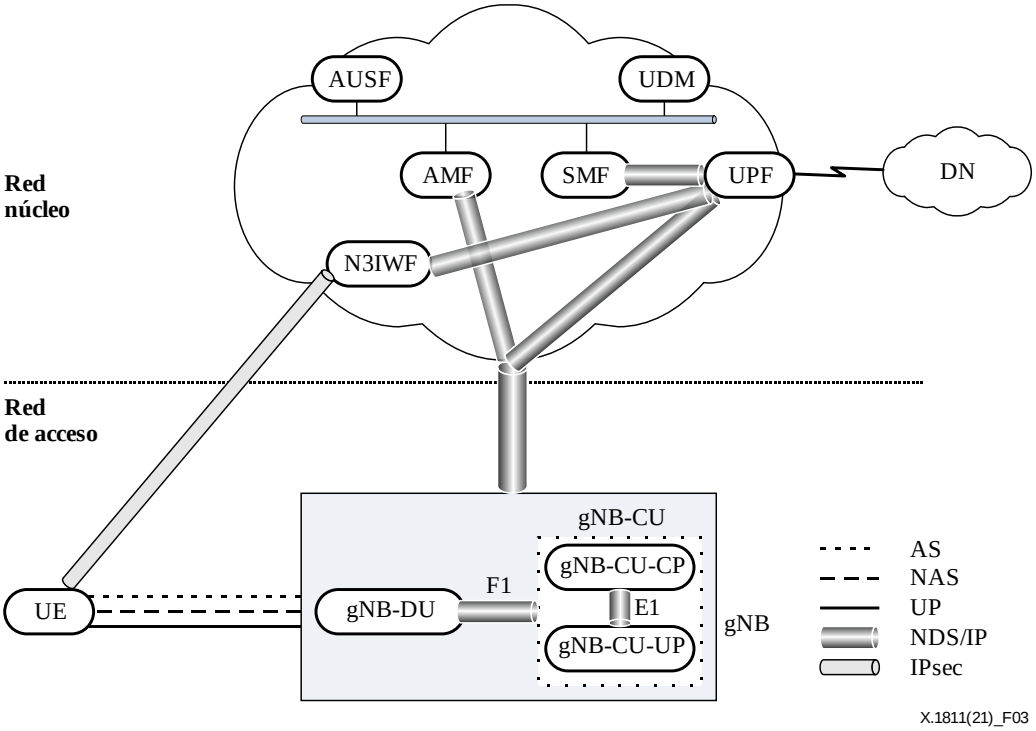

Figura 3 – Arquitectura de seguridad de la red de acceso

7.2.1.1 Privacidad del abonado

Al EU se le asigna un identificador de abono permanente (SUPI, *subscription permanent identifier*) exclusivo a nivel mundial en el sistema IMT-2020, que se configurará en el módulo universal de identidad de abonado (USIM, *universal subscriber identity module*) y en la gestión de datos unificados/repositorio de datos de usuario (UDM/UDR, *unified data management/user data repository*). Un SUPI nunca se transmite sin encriptar por una interfaz inalámbrica cuando hay un USIM IMT-2020 desplegado. Para el acceso inicial, el EU genera un identificador de abono oculto (SUCI, *subscription concealed identifier*) y lo transmite a la gestión de datos unificados/función repositorio y procesamiento de credenciales de autentificación (UDM/ARPF, *unified data management/authentication credential repository and processing function*), como se muestra en la Figura 4. Al recibir un SUCI, la función revelación del identificador de abono (SIDF, *subscription identifier de-concealing function*) ubicada en la ARPF/UDM procede a la revelación del SUPI a partir del SUCI. En función del SUPI, la UDM/ARPF escoge el método de autentificación acorde con los datos del abono.

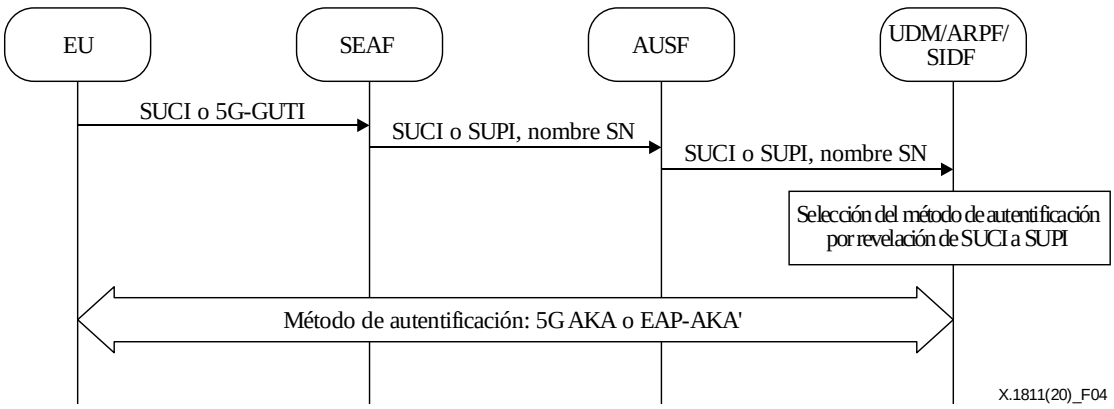

Figura 4 – Procedimiento de autentificación inicial y selección del método de autentificación (adaptado de la Figura 6.1.2-1 de [b-3GPP TS 33.501])

Un SUCI se compone de una parte encriptada y una parte no encriptada. La parte no encriptada contiene el indicativo de país móvil y el código de red móvil como información perteneciente a la red de origen para el encaminamiento del SUCI a la UDM/ARPF objetivo. La parte encriptada contiene información sensible sobre el abono, como el número de identificación móvil, que se encripta utilizando el esquema de encriptación integrado de curva elíptica (ECIES, *elliptic curve integrated encryption scheme*). La clave pública de la red de origen está configurada de manera segura en el USIM y la SIDF, respectivamente. El principio del ECIES es que el EU y la red aplican sus propias claves privada y pública asociada para acordar las claves compartidas utilizando el mecanismo ECDH. De acuerdo con las claves compartidas se procede a la protección de la confidencialidad y la integridad de los datos utilizando algoritmos de encriptación simétricos y algoritmos MAC, respectivamente. De acuerdo con los perfiles especificados en [b-3GPP TS 33.501], se utilizan mecanismos ECDH (X25519, primitiva DH cofactorial de curva elíptica) para generar las claves compartidas, y AES-128 en modo contador y HMAC-SHA-256 respectivamente para la confidencialidad de los datos y la integridad de los datos.

Una vez iniciado el procedimiento de autentificación, se asigna de manera segura al EU un identificador temporal exclusivo a nivel mundial IMT-2020 (IMT-2020-GUTI, *IMT-2020 globally unique temporary identifier*) para ocultar el SUPI en el procedimiento de autentificación subsiguiente.

7.2.1.2 Autentificación

Los sistemas IMT-2020 aplican dos tipos de protocolo AKA para la autentificación mutua entre el EU y la red, además de la generación de la clave de sesión, K_{SEAF}. Se trata de IMT-2020-AKA y de protocolo de autentificación extensible-protocolo de autentificación y acuerdo de clave (EAP-AKA', *extensible authentication protocol-authentication and key agreement*). Este último puede utilizarse para el acceso 3GPP y no 3GPP. En comparación con los utilizados en la 4G, los protocolos de autentificación IMT-2020 aumentan el control en origen para paliar cualquier posible tarificación fraudulenta de la red visitada. En el caso de EAP-AKA', la verificación de la identidad del EU en el lado red se ejecuta en la función servidor de autentificación (AUSF, *authentication server function*) de la red de origen. En el caso de IMT-2020-AKA, aunque la verificación de la identidad del EU en el lado red se efectúa en la función anclaje de seguridad (SEAF, *security anchor function*) de la red visitada, la AUSF de la red de origen verificará la confirmación de autentificación durante cada fase del procedimiento de autentificación.

En el procedimiento de autentificación se utiliza una serie de algoritmos de generación de claves (*f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 y *f*5*) para generar el vector de autentificación (AV, *authentication vector*) y la respuesta de autentificación. Hay dos tipos de series de algoritmos válidos para ello. El primero se denomina serie de algoritmos MILENAGE [b-ETSI 135 205], cuya base recomendada es AES-128. La segunda se denomina serie de algoritmos TUAK [b-ETSI 135 231], cuya base es la función esponja de Keccak [b-Bertoni] y donde las claves de entrada pueden ser de 128 bits o de 256 bits. Téngase en cuenta que, en la práctica, se utiliza con más frecuencia la serie de algoritmos MILENAGE que la serie TUAK.

7.2.1.3 Jerarquía de claves

Sobre la base de la clave raíz, K, el EU y la red proceden a la autentificación mutua y generan la clave de la sesión, K_{SEAF}, que es el ancla de las claves (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) utilizadas para asegurar la comunicación entre el EU y la red, como se muestra en la Figura 5.

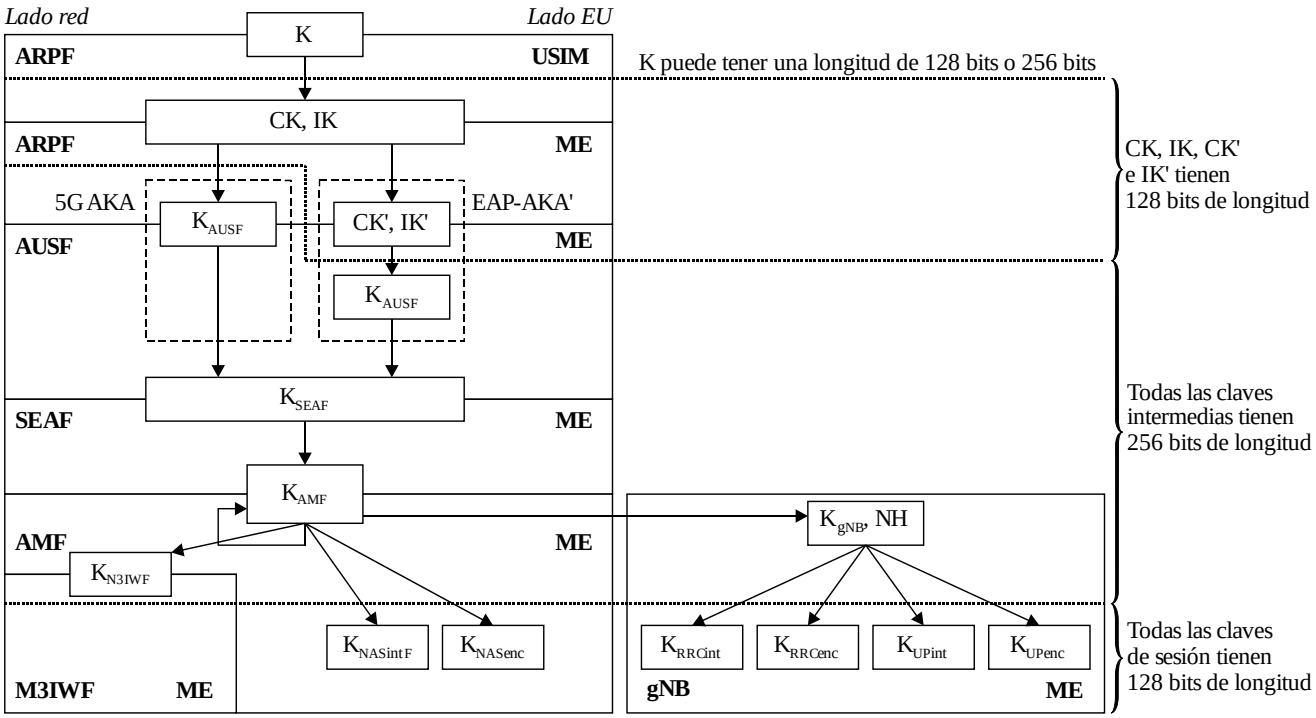

Figura 5 – Jerarquía de claves (adaptada de la Figura 6.2.1-1 de [b-3GPP TS 33.501])

La clave raíz, K, puede tener 128 o 256 bits de longitud. Cabe señalar que la clave raíz, K, en el USIM heredado sólo tiene 128 bits de longitud, lo que significa que para ese USIM en el UDM sólo pueden configurarse claves raíz de 128 bits de longitud.

CK, IK, CK' e IK' son las claves relacionadas con el procedimiento de autentificación y su longitud es de 128 bits. La generación de CK e IK depende de la serie de algoritmos MILENAGE o TUAK, mientras que para producir CK' e IK' se utiliza la función derivación de clave genérica (GKDF, *generic key derivation function*) definida en [b-3GPP TS 33.220].

Todas las claves intermedias tienen 256 bits de longitud y su generación depende de GKDF a excepción de la clave K_{AUSF} en el protocolo EAP-AKA'. La función derivación de claves por extracción y expansión basada en HMAC (HKDF, *HMAC-based extract-and-expand key derivation function*), especificada en [b-IETF RFC 5869], se utiliza para generar la clave K_{AUSF} en el protocolo EAP-AKA'.

Las claves (K_{N3IWF}, K_{NASint}, K_{NASenc}, K_{RRCint}, K_{RRCenc}, K_{UPint}, K_{UPenc}) utilizadas para asegurar la comunicación entre el EU y la red tienen 128 bits de longitud y son resultado del truncamiento del resultado de 256 bits de GKDF.

7.2.1.4 Seguridad de la señalización NAS, la señalización AS y los datos de usuario

Para garantizar la confidencialidad de la señalización NAS, la señalización AS y los datos de usuario, los sistemas IMT-2020 soportarán 128-NEA1 (algoritmo basado en SNOW 3G de 128 bits) y 128-NEA2 (algoritmo basado en AES de 128 bits). Además, los sistemas IMT-2020 podrán soportar 128-NEA3 (algoritmo basado en ZUC de 128 bits).

Para garantizar la integridad de la señalización NAS, la señalización AS y los datos de usuario, los sistemas IMT-2020 deberán soportar 128-NIA1 (algoritmo basado en SNOW 3G de 128 bits) y 128-NIA2 (algoritmo basado en AES de 128 bits). Además, los sistemas IMT-2020 podrán soportar 128-NIA3 (algoritmo basado en ZUC de 128 bits).

7.2.1.5 NDS/IP

Las interfaces entre la red de acceso y la red núcleo (es decir, interfaz N2 entre gNB y AMF, interfaz N2 entre N3IWF y AMF, interfaz N3 entre gNB y UPF, interfaz N3 entre N3IWF y UPF), las interfaces entre gNB-DU y gNB-CU (interfaz F1), y las interfaces entre gNB-CU-CP y gNB-CU-UP (interfaz E1) se protegen con NDS/IP ([b-3GPP TS 33.210], [b-3GPP TS 33.310]), que especifica el perfil de seguridad utilizado en los sistemas 3GPP para IPsec, intercambio de claves Internet versión 2 (IKEv2, *Internet key exchange version 2*), TLS y seguridad de la capa de transporte de datagramas (DTLS, *datagram transport layer security*) [b-IETF RFC 6083].

Para proteger la integridad y la confidencialidad de los datos transmitidos por la interfaz N2, la interfaz E1 y la interfaz F1, así como para prevenir ataques de reproducción, se recomienda utilizar la autentificación basada en certificados de la carga útil de seguridad de encapsulado (ESP, *encapsulating security payload*) IPSec e IKEv2. Además, deberá soportarse DTLS.

Para garantizar la integridad, la confidencialidad y la protección de respuesta del tráfico por la interfaz N3, se recomienda utilizar la autentificación basada en certificados ESP IPsec e IKEv2.

Además de AES-256, se deberán soportar los algoritmos de encriptación ESP, la norma de encriptación avanzada-encadenamiento de bloques cifrados (AES-CBC, *advanced encryption standard-cipher blocker chaining*) y la norma de encriptación avanzada-modo contador de Galois (AES-GCM, *advanced encryption standard-Galois counter mode*) con un ICV de 16 octetos. Como algoritmos de autentificación ESP, se deberán soportar HMAC-SHA1-96 y la norma de encriptación avanzada-código de autentificación de mensaje de Galois (AES-GMAC, *advanced encryption standard-Galois message authentication code*) con AES-128.

En relación con IKEv2, deberán soportarse los algoritmos siguientes:

– confidencialidad: ENCR_AES_CBC con una clave de 128 bits, AES-GCM con un ICV de 16 octetos con una clave de 128 bits;

– función pseudoaleatoria: PRF_HMAC_SHA1, PRF_HMAC_SHA2_256;

– integridad: AUTH_HMAC_SHA256_128;

– DH group 14 (MODP de 2 048 bits),19 (grupo ECP aleatorio de 256 bits).

En relación con IKEv2, para una seguridad de alto nivel deben soportarse los algoritmos siguientes:

– confidencialidad: AES-GCM con un ICV de 16 octetos con una clave de 256 bits;

– función pseudoaleatoria: PRF_HMAC_SHA2_384;

– DH group 20 (grupo ECP aleatorio de 384 bits).

DTLS 1.2 comparte las mismas series cifradas que TLS 1.2, pues DTLS 1.2, como se especifica en [b-IETF RFC 6347], se basa en TLS 1.2. Se utilizarán las series cifradas permitidas y obligatorias determinadas en TLS 1.2 [b-IETF RFC 5246]. Además, se han de soportar las siguientes series cifradas cuya utilización se recomienda:

– TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, como se define en [b-IETF RFC 5289];

– TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, como se define en [b-IETF RFC 5288].

Para una seguridad de alto nivel se recomienda el soporte de las siguientes series cifradas:

– TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, como se define en [b-IETF RFC 5289];

– TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 como se define en [b-IETF RFC 5289].

En cuanto a los grupos DH, para ECDHE, se deberá soportar la curva secp256r1 (P-256) definida en [b-IETF RFC 4492] y se debe soportar secp384r1 (P-384) definida en [b-IETF RFC 4492]. Para DHE, deben soportarse grupos DH de al menos 4 096 bits. No se soportarán grupos DH de menos de 2 048 bits.

La autentificación PSK puede utilizarse en IKEv2, y el contacto TLS en el contexto de NDS/IP.

7.2.1.6 Seguridad del acceso no 3GPP

La seguridad del acceso no 3GPP se logra estableciendo un túnel IPsec entre el EU y N3IWF. IKEv2 [b-IETF RFC 7296] se utiliza para efectuar la autentificación mutua entre el EU y N3IWF sobre la base de la clave K_{N3IWF} para crear una o más asociaciones de seguridad ESP IPsec [b-IETF RFC 4303] para los túneles IPsec.

La seguridad de la comunicación entre N3IWF y AMF (interfaz N2), así como entre N3IWF y UPF (interfaz N3) se logra con NDS/IP.

7.2.2 Seguridad de la red núcleo

Se prevé que la red núcleo IMT-2020 se construya sobre la base de un marco NFV [b-ETSI GS NFV 002], donde las funciones de red (NF) se disocien del *hardware* dedicado para un despliegue de servicio rápido y una mayor eficiencia operativa. Como se muestra en la Figura 6, el marco NFV puede dividirse en tres capas: NFVI, VNF y servicios de red. Las VNF se ejecutan sobre la capa NFVI común para ofrecer los servicios de red deseados. La seguridad de la red núcleo es esencialmente la de la capa VNF.

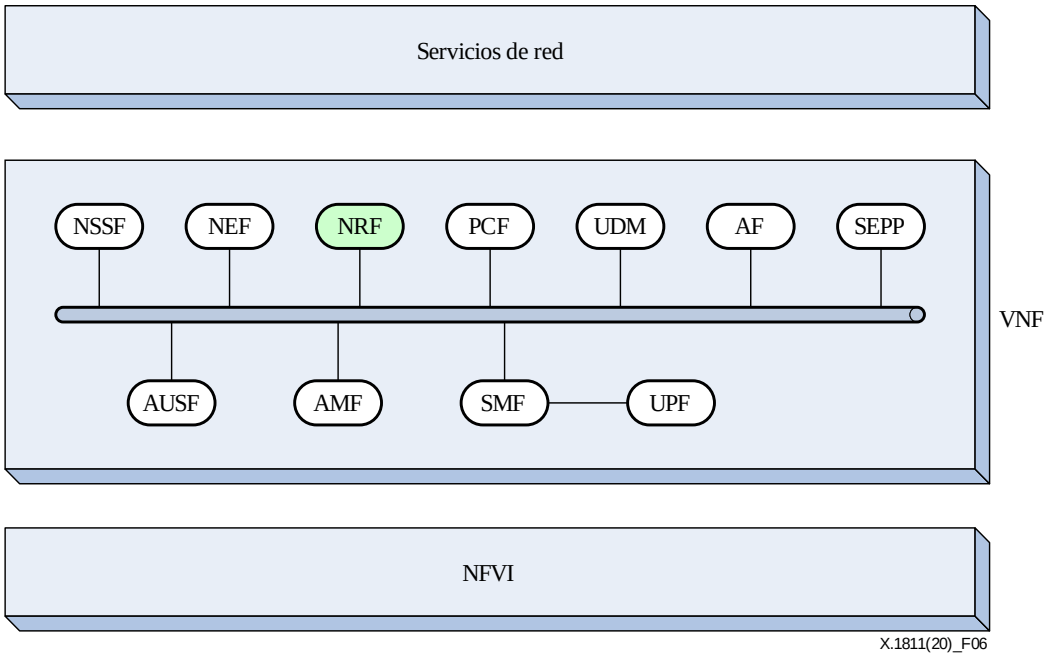

Figura 6 – Marco de la red núcleo IMT-2020 basada en NFV (adaptado de la Figura 1 de [b-ETSI GS NFV 002])

Las VNF se organizan en una SBA, donde la función repositorio NF (NRF, *NF repository function*) desempeña un papel fundamental en el sistema. La NRF decide si una NF está autorizada para proceder al descubrimiento y el registro, y expide un testigo de acceso a la NF. La seguridad de las capas VNF puede considerarse dentro de una red pública móvil terrestre (RPMT) o entre las RPMT.

7.2.2.1 Dentro de una RPMT

1) Autentificación

La NRF y la NF se autentificarán mutuamente durante el proceso de descubrimiento, registro y solicitud de testigo de acceso, lo que puede efectuarse utilizando NDS/IP o seguridad física. La autentificación entre NF puede efectuarse de la misma manera.

2) Autorización

– Autorización estática

Una vez que la NF del consumidor de servicios y la NF del productor de servicios se autentifican mutuamente, la NF del productor de servicios verificará la autorización de la NF del consumidor de servicios de acuerdo con la política local antes de concederle el acceso a la interfaz de programación de aplicaciones (API, *application programming interface*) del servicio.

– **Autorización basada en OAuth 2.0**

El control de acceso a los servicios de red prestados por las NF puede efectuarse utilizando un marco OAuth 2.0, como se especifica en [b-IETF RFC 6749]. Los testigos de acceso serán testigos web en notación de objeto JavaScript (JSON, *JavaScript object notation*), descritos en [b-IETF RFC 7519], asegurados con firmas digitales o firmas digitales MAC basadas en una firma web JSON (JWS, *JSON web signature*), como se indica en [b-IETF RFC 7515]. La NRF actúa como un servidor de autorización OAuth 2.0. El consumidor de servicios NF y el productor de servicios NF corresponden respectivamente al cliente OAuth 2.0 y el servidor de recursos OAuth 2.0. La comunicación entre las NF y la NRF se protege con TLS, pues se transmiten credenciales entre ellas.

7.2.2.2 Entre RPMT

La seguridad entre RPMT se logra gracias a los intermediarios de protección del perímetro de seguridad (SEPP, *security edge protection proxies*) de ambas redes a través de una interfaz N32, como se muestra en la Figura 7.

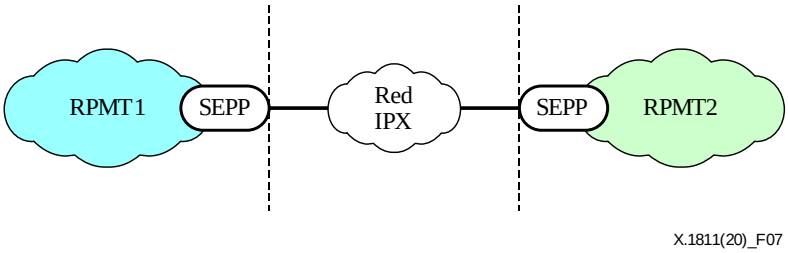

Figura 7 – Seguridad entre RPMT

La interfaz N32 consta de una conexión N32-c y una conexión N32-f. La primera es responsable de la gestión de la interfaz N32, incluida la AKA mutua entre dos SEPP utilizando TLS. La segunda sirve para enviar mensajes protegidos con firma y encriptación de objetos JavaScript (JOSE, *Javascript object signing and encryption*) entre los SEPP.

Los SEPP utilizan la encriptación web JSON (JWE, especificada en [b-IETF RFC 7516]) para proteger los mensajes en la interfaz N32, donde se aplican las claves acordadas entre dos SEPP en la conexión N32-c. Los proveedores de centrales IP (IPX, *IP exchange*) aplican la JWS especificada en [b-IETF RFC 7515] para firmar las modificaciones necesarias para sus servicios de mediación.

Todas las entidades y funciones que soportan la JWE utilizarán los siguientes algoritmos [b-3GPP-TS 33.210]: se deberá soportar "enc" parameter A128GCM (AES-GCM con una clave de 128 bits); se debe soportar "enc" parameter A256GCM (AES-GCM con una clave de 256 bits); se deberá soportar "alg" parameter "dir" (utilización directa de una clave simétrica compartida como clave de encriptación de contenido (CEK, *content encryption key*)).

Todas las entidades y funciones que soportan JWS deberán soportar los siguientes algoritmos [b-3GPP-TS 33.210]: se deberá soportar "alg" parameter ES256 (algoritmo de firma digital de curva elíptica (ECDSA, *elliptic curve digital signature algorithm*) con P-256 y algoritmo de número generador seguro-256 (SHA-256, *secure hash algorithm-256*)).

7.3 Seguridad del plano de gestión

El plano de gestión está compuesto por un conjunto gestor (orquestador NFV, gestor VNF, gestor de infraestructura virtualizada, controlador SDN, gestor RAN). Este conjunto gestor se ocupa de la gestión de la configuración, la calidad de funcionamiento y los fallos de los objetivos correspondientes a través de las interfaces. Deberá evitarse toda modificación, supresión, inserción o reproducción durante la transferencia de datos entre el gestor y el objetivo gestionado [b-ETSI GS NFV-SEC 014]. Para ello, se aplica la TLS a estas interfaces por defecto en fábrica, como se muestra en la Figura 8.

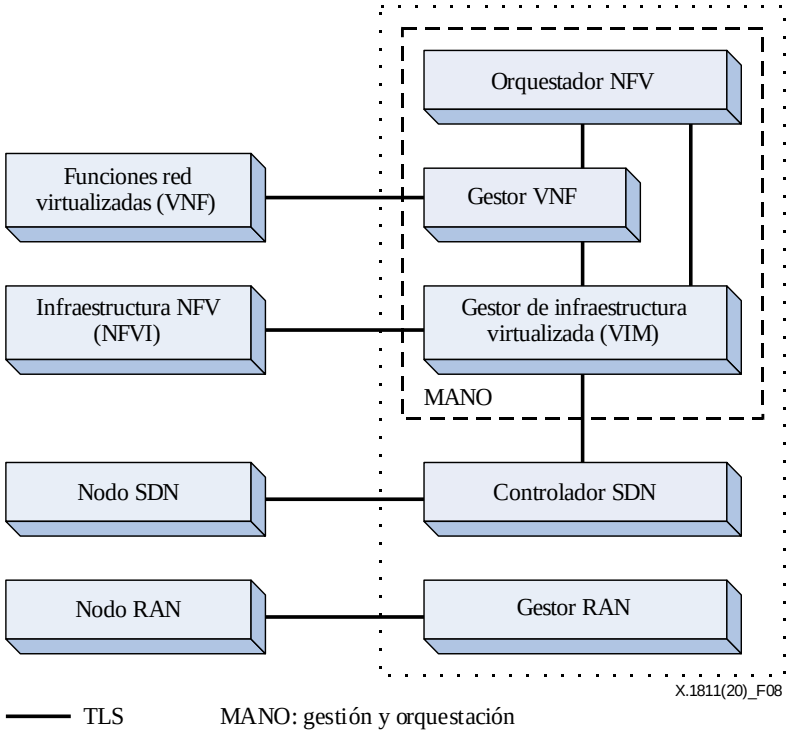

Figura 8 – Seguridad del plano de gestión

7.4 Resumen de los algoritmos criptográficos utilizados en sistemas IMT-2020

De acuerdo con la introducción a la arquitectura de seguridad de sistemas IMT-2020 expuesta en las cláusulas 7.1 a 7.3, en el Cuadro 1 se resumen los algoritmos criptográficos utilizados en sistemas IMT-2020.

Cuadro 1 – Algoritmos criptográficos utilizados en sistemas IMT-2020

Tipo	Nombre	Función	Situación de aplicación
Algoritmos criptográficos simétricos	128-NEA1	Encriptación	Protección de la confidencialidad entre el EU y la AMF, así como entre el EU y el gNB
	128-NEA2		
	128-NEA3		
	128-NIA1	MAC	Protección de la integridad entre el EU y la AMF, así como entre el EU y el gNB
	128-NIA2		
	128-NIA3		
	AES-128	Encriptación	IPsec, TLS, DTLS, JWE, ECIES, NFVI
	AES-256	Encriptación	IPsec, TLS, DTLS, JWE, NFVI
	Blowfish	Encriptación	SDN
	3DES	Encriptación	SDN
	SHA-256	Troceo	IPsec, TLS, DTLS, JWS, NFVI
	SHA-384	Troceo	IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-256	Derivación de claves/MAC/función pseudoaleatoria	Jerarquía de claves IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-384	Derivación de claves/MAC/función pseudoaleatoria	IPsec, TLS, DTLS, JWS, NFVI
Algoritmos criptográficos asimétricos	RSA	Firma	IPsec, TLS, DTLS, JWS, NFVI
	ECDSA	Firma	IPsec, TLS, DTLS, JWS, NFVI
	DH	Acuerdo de claves	IPsec, TLS, DTLS, NFVI
	ECDH	Acuerdo de claves	IPsec, TLS, DTLS, NFVI

NOTA 1 – SHA-1 no figura en la lista por su escasa solidez de seguridad.

NOTA 2 – No se indica la longitud de las claves utilizadas en los algoritmos criptográficos asimétricos, pues éstos podrían vencerse, independientemente del tamaño de la clave, de haber ordenadores cuánticos a gran escala.

NOTA 3 – Por motivos de seguridad la versión de TLS no deberá ser inferior a 1.2.

8 Evaluación de la seguridad de los sistemas IMT-2020 ante la informática cuántica

Un ordenador cuántico es un dispositivo que explota los fenómenos mecánicos cuánticos (superposición y entrelazamiento) para realizar cálculos y manipular datos. Los fundamentos de la seguridad de los algoritmos criptográficos actualmente utilizados se basa en problemas matemáticos inextricables. Dado el paralelismo intrínseco de los ordenadores cuánticos, algunos algoritmos cuánticos pueden resolver problemas matemáticos difíciles más eficazmente que los algoritmos clásicos, lo que supone una seria y verosímil amenaza para la seguridad de la criptografía contemporánea. En el Apéndice III se indican las consecuencias de la informática cuántica para los algoritmos criptográficos comunes. En la cláusula 8.1 se presentan las amenazas que la disponibilidad de ordenadores cuánticos supone para los algoritmos criptográficos convencionales. A continuación se analizan las consecuencias de los ordenadores cuánticos para los sistemas IMT-2020.

8.1 Amenazas a los algoritmos criptográficos convencionales

8.1.1 Algoritmos criptográficos asimétricos

El algoritmo de Shor puede solucionar el problema de factorización de enteros grandes y el problema de logaritmo discreto en un tiempo polinómico [b-Shor 1999], lo que mina la seguridad de los algoritmos asimétricos actualmente utilizados. Esto significa que la criptografía de clave pública basada en RSA, cuya seguridad se basa en el problema de factorización de enteros grandes, y el protocolo de intercambio de claves DH, cuya seguridad se basa en el problema de logaritmo discreto, no ofrecerán seguridad alguna. Al igual que el algoritmo DH, la seguridad del algoritmo DSA depende del logaritmo discreto. Por consiguiente, el algoritmo DSA puede ser objeto de ataques cuánticos. ECC, cuya seguridad depende del problema de logaritmo discreto de curva elíptica (ECDLP, *elliptic curve discrete-log problem*), se ha utilizado profusamente, pues su clave tiene un tamaño notablemente menor que la del sistema de clave pública basada en RSA. Sin embargo, es posible vencerlo utilizando una variante del algoritmo de Shor [b-Roetteler]. Esto implica que ECC, incluidos ECDSA y ECDH, no son seguros en presencia de ordenadores cuánticos a gran escala. En el Cuadro 2 se indican los recursos cuánticos necesarios para vencer los algoritmos criptográficos asimétricos que tanto se utilizan hoy en día.

Cuadro 2 – Recursos cuánticos necesarios para vencer los algoritmos criptográficos asimétricos

Algoritmos	Tamaño de clave pública (bits)	Nivel de seguridad comparable al de algoritmo simétrico (bits)	Qubits lógicos	Qubits físicos (véase la Nota 1)	Puertas de Toffoli (véase la Nota 1)	Tiempo necesario para vencer los algoritmos (véase la Nota 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 días y 14 h
	4 096	128	8 194	$2{,}95 \times 10^{7}$	$5{,}59 \times 10^{13}$	31 días y 21 h
Basado en 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

NOTA 1 – Los ordenadores cuánticos necesitan más bits cuánticos físicos para la corrección de errores. El número de qubits físicos por qubit lógico varía entre 10 y 10 000. Suponemos aquí un qubit lógico por 3 600 qubits físicos, véase [b-Fowler].

NOTA 2 – Se supone que el tiempo operativo de una puerta de Toffoli es de 60 ns, véase [b-Banchi].

8.1.2 Algoritmos criptográficos simétricos

El algoritmo de Grover acelera cuadráticamente las búsquedas en conjuntos de datos no estructurados en comparación con los algoritmos clásicos [b-Grover]. Esto puede servir para buscar la clave en el espacio de claves de un algoritmo de clave simétrica. En el caso de un algoritmo de clave simétrica cuya clave tenga n bits de longitud, la clave puede encontrarse en $O(2^{n/2})$ operaciones cuánticas efectuadas por la máquina cuántica, en lugar de las $O(2^{n})$ operaciones clásicas de una computadora convencional. Los recursos cuánticos necesarios para buscar la clave de un algoritmo simétrico son tan elevados que puede ponerse en duda la ejecución del algoritmo de Grover para vencer un algoritmo de clave simétrica en un ordenador cuántico físico real. Por ejemplo, una búsqueda exhaustiva de las claves de un AES utilizando el algoritmo de Grover necesita el siguiente número de puertas de Toffoli y de Clifford: 2^{86} para AES-128; 2^{118} para AES-192, y 2^{151} para AES-256, aunque el número de qubits lógicos necesarios oscila entre 3 000 y 7 000 [b-Grassl].

El algoritmo de Grover divide la longitud efectiva de la clave entre dos, es decir, divide entre dos la solidez de seguridad de un algoritmo de clave simétrica. Por tanto, para lograr la resistencia cuántica es necesario duplicar el tamaño de la clave del algoritmo de clave simétrica.

8.1.3 Algoritmos de troceo

El algoritmo de Grover y sus variantes no permiten encontrar más rápidamente las colisiones de troceo que los algoritmos clásicos [b-Bernstein 2009]. El mejor método sería utilizar una versión paralela del método ρ de Pollard en un conjunto de computadoras clásicas [b-ETSI GR QSC 006]. Esto significa que, si los algoritmos de troceo actualmente utilizados son seguros, serán seguros contra los ataques informáticos cuánticos en la era cuántica. Se ha demostrado que SHA-256 es seguro en la informática clásica y que también podrá resistir a un ataque de preimagen cuántico [b-Amy].

8.1.4 Funciones de derivación de claves

El objetivo de las funciones derivación de claves (KDF, *Key derivation functions*) es generar las claves utilizadas para la protección de la confidencialidad y la integridad, lo que se logra incorporando la clave compartida en las funciones de troceo. Hay dos tipos de KDF en los sistemas IMT-2020. El primero es la GKDF definida en [b-3GPP TS 33.220] y el segundo es la HKDF especificada en [b-IETF RFC 5869].

La base de la GKDF y la HKDF es la función de troceo de claves HMAC-SHA-256. La seguridad de HMAC depende de la solidez criptográfica de la función de troceo utilizada [b-IETF RFC 2104]. Por consiguiente, las KDF utilizadas en los sistemas IMT-2020 no se ven sustancialmente afectadas por los avances de la informática cuántica.

Téngase en cuenta que la entropía del resultado de las KDF depende de la entropía de la clave de entrada utilizada en las KDF. Para un resultado de entropía de 256 bits se necesita una clave de entrada de entropía de 256 bits al aplicar las KDF.

8.2 Predicción sobre la disponibilidad de ordenadores cuánticos a gran escala

Resulta difícil predecir cuándo exactamente estarán disponibles los ordenadores cuánticos a gran escala, porque no hay un consenso al respecto. En [b-NISTIR 8105] se estima que un ordenador cuántico de 1 000 millones USD pueda vencer un RSA de 2 048 bits en 2030. El Instituto Europeo de Normas de Telecomunicaciones (ETSI) ha llegado del mismo modo a la conclusión de que en 2031 puedan construirse ordenadores cuánticos a gran escala [b-ETSI GR QSC 004]. Por consiguiente, la seguridad de los sistemas IMT-2020 podrá verse en peligro, pues éstos operarán durante un periodo de entre 10 y 20 años. Por otra parte, [b-NASEM] considera muy improbable que pueda construirse un ordenador cuántico capaz de vencer un RSA de 2 048 bits durante la próxima década, lo que no implica que los algoritmos criptográficos de seguridad cuántica no deban estudiarse y normalizarse ahora, pues el tiempo que llevará la transición a un nuevo algoritmo de seguridad será largo y difícil de definir [b-NASEM].

8.3 Repercusiones para los sistemas IMT-2020

Como se indica en la cláusula 7, IPsec, TLS y DTLS se han desplegado profusamente en las redes IMT-2020. En primer lugar es necesario tener una visión de conjunto para evaluar las amenazas que representan los ordenadores cuánticos. A continuación, se evaluarán las repercusiones para la seguridad de los sistemas IMT-2020 de acuerdo con la estructura presentada en la cláusula 7.

8.3.1 Repercusiones para IPsec, TLS y DTLS

Aunque IPsec, TLS y DTLS se ejecutan en distintas capas para proteger la transmisión de los mensajes (IPSec reside en la capa de red, mientras que TLS y DTLS residen entre las capas de red y de aplicación), su diseño se ajusta a un principio similar. Se componen de dos partes: la primera es la autentificación y el establecimiento de claves para generar claves de sesión; la segunda es la

protección de la confidencialidad y la integridad de los mensajes utilizando algoritmos simétricos con las claves de sesión.

Hay dos métodos para realizar la autentificación y el establecimiento de claves, que se basan en (1) una clave simétrica precompartida o (2) una clave pública (generalmente se utiliza un certificado).

Para la protección de la confidencialidad y la integridad, las series cifradas actuales de IPsec, TLS y DTLS pueden soportar algoritmos simétricos tanto de 128 bits como de 256 bits.

Por consiguiente, es posible evaluar si IPsec, TLS y DTLS pueden soportar ataques informáticos cuánticos contemplando los casos 1 a 4.

Caso 1: Autentificación por clave pública y algoritmos simétricos de 128 bits o 256 bits

En este caso, los atacantes pueden recuperar las claves de sesión, pues los algoritmos asimétricos actualmente especificados en las normas del Grupo de Tareas sobre Ingeniería de Internet (IETF) pueden ser vencidos por los ordenadores cuánticos gracias al algoritmo de Shor. Por tanto, independientemente de la longitud de la clave de los algoritmos simétricos, no puede garantizarse la seguridad de los mensajes transmitidos.

Caso 2: Autentificación por PSK de 128 bits y algoritmos simétricos de 128 bits

En este caso, a causa del algoritmo de Grover, el tamaño efectivo de la clave de seguridad es 64 bits en presencia de un ordenador cuántico a gran escala. Por consiguiente, estos tres protocolos no son seguros en caso de ataque cuántico.

Caso 3: Autentificación por PSK de 256 bits y algoritmos simétricos de 128 bits

En este caso, aunque se utiliza una PSK de 256 bits para la autentificación y el establecimiento de claves, sólo se aplican algoritmos simétricos de 128 bits para la protección de los mensajes. Así, la solidez de seguridad de estos tres protocolos es de 64 bits.

Caso 4: Autentificación por PSK de 256 bits y algoritmos simétricos de 256 bits

En este caso, la solidez de seguridad efectiva de estos tres protocolos es de 128 bits, por lo que es posible frustrar ataques cuánticos utilizando este perfil de cifrado.

De los perfiles de cifrado actuales, sólo el caso 4 es seguro en caso de ataque cuántico. Sin embargo, la autentificación por PSK sólo es adecuada para un pequeño grupo de comunicación, pues una PSK debe configurarse manualmente en cada uno de los dispositivos utilizados. Se recomienda utilizar la autentificación por clave pública cuando el grupo de comunicación se amplía. Para ello, se recomienda introducir en los protocolos mencionados para la autentificación (a saber, IPSec, TLS y DTLS) algoritmos asimétricos criptográficos de seguridad cuántica.

8.3.2 Repercusiones para la capa de infraestructura

Como se muestra en la cláusula 7.1, TLS se utiliza para proteger la interfaz entre las aplicaciones y el controlador SDN, así como en la interfaz entre el controlador SDN y los nodos SDN. Puede utilizarse IPsec en la interfaz entre el controlador SDN y los nodos SDN. De acuerdo con los análisis de la cláusula 8.3.1, estas dos interfaces son objeto de ataques cuánticos, es decir, que los atacantes pueden interceptar, alterar e inyectar los mensajes transmitidos entre estas dos interfaces a menos que se introduzcan en TLS e IPSec los algoritmos del caso 4.

La capa NFVI es vulnerable a los ataques cuánticos, pues algunas de sus funciones de seguridad dependen de algoritmos criptográficos asimétricos clásicos, lo que puede tener consecuencias graves, como el acceso ilegal a la plataforma o la instalación de *software* maligno.

8.3.3 Repercusiones para la red de acceso

8.3.3.1 Privacidad del abonado

Un SUPI se oculta convirtiéndolo en SUCI según el esquema ECIES presentado en la cláusula 7.2, y se utiliza el ECDH para acordar y compartir la clave entre el EU y la red. Los atacantes pueden recuperar la clave compartida gracias al algoritmo de Shor, en caso de contar con ordenadores cuánticos a gran escala. Por consiguiente, los atacantes pueden conocer el SUPI descifrando el SUCI con la clave compartida.

8.3.3.2 Autentificación

Tanto el protocolo IMT-2020 AKA como el protocolo EAP-AKA' efectúan la autentificación mutua entre el EU y la red sobre la base de la clave a largo plazo K, cuyo tamaño puede ser de 128 bits o de 256 bits. Con la clave K de 256 bits hasta la fecha no ha habido ataques a las funciones de troceo (es decir, la serie de algoritmos TUAK) que son la base de la que se derivan diversos parámetros utilizados en el protocolo de autentificación con un ordenador clásico. Por consiguiente, ambos protocolos de autentificación son seguros contra los ataques cuánticos, pues no hay ningún algoritmo más eficaz para vencer las funciones de troceo con ordenadores cuánticos que los que ya se utilizan con ordenadores clásicos en el contexto de una clave K de 256 bits. Con una clave K de 128 bits, cuya solidez de seguridad efectiva es de 64 bits en la era cuántica, los atacantes pueden recuperar la clave K de los mensajes capturados relacionados con ambos protocolos de autentificación, por ejemplo, AV realizando 2^{64} operaciones cuánticas utilizando el algoritmo de Grover.

8.3.3.3 Jerarquía de claves

La jerarquía de claves se utiliza para derivar claves de 128 bits a partir de la clave a largo plazo (raíz) K, como se muestra en la Figura 5, a fin de proteger la comunicación entre el EU y la red. En la actualidad se utiliza ampliamente la clave K de 128 bits, mientras que la clave K de 256 bits se utiliza muy poco. Con una clave K de 128 bits, cuya solidez de seguridad efectiva es de 64 bits en la era cuántica, la solidez de seguridad de las claves derivadas es de 64 bits. Por consiguiente, los atacantes pueden recuperar las claves a partir de los mensajes encriptados con claves de 128 bits capturados.

8.3.3.4 Señalización NAS, señalización AS y datos de usuario

La confidencialidad de la señalización NAS, la señalización AS y los datos de usuario se protegen con algoritmos simétricos y claves de 128 bits de longitud. Por tanto, los atacantes pueden desencriptar esos mensajes utilizando ordenadores cuánticos.

La integridad de la señalización NAS, la señalización AS y los datos de usuario se protege con algoritmos MAC y una clave de 128 bits de longitud. El resultado de los algoritmos MAC se trunca en etiquetas de 32 bits de longitud utilizadas como etiquetas MAC. Un atacante puede directamente falsificar un mensaje tras 231 intentos, si la etiqueta MAC tiene 32 bits de longitud. Queda en estudio si la seguridad de un sistema IMT-2020 corre riesgos si la etiqueta MAC de 32 bits se ha truncado de una etiqueta nativa de 64 bits o de una etiqueta nativa de 128 bits.

8.3.3.5 NDS/IP

TLS, DTLS e IPsec se utilizan para proteger la interfaz N2, la interfaz N3, la interfaz E1 y la interfaz F1, como se explica en la cláusula 7.2.1. Las repercusiones son las mismas que para la capa de transporte, a saber, los atacantes pueden interceptar, alterar e inyectar los mensajes transmitidos por esas interfaces si no se utiliza el cifrado del caso 4 de la cláusula 8.3.1.

8.3.3.6 Seguridad del acceso no 3GPP

El acceso no 3GPP se asegura con IPsec. Por los motivos indicados en la cláusula 8.3.1, no es posible garantizar la seguridad del acceso no 3GPP a menos que se utilice el cifrado del caso 4 de la cláusula 8.3.1.

8.3.4 Repercusiones para la red núcleo

8.3.4.1 Dentro de una RPMT

1) Autentificación

La autentificación entre NF no se verá afectada si su funcionamiento depende de seguridad física. La autentificación puede ser objeto de las mismas amenazas especificadas en la cláusula 8.3.3 si se efectúa mediante NDS/IP.

2) Autorización

La autorización estática no se verá afectada, pues no se aplican algoritmos criptográficos.

En el caso de la autorización por OAuth 2.0 hay dos posibles maneras de garantizar la integridad del testigo de acceso. El adversario puede falsificar un testigo de acceso si su integridad está protegida con una firma. Por el contrario, es imposible falsificar un testigo de acceso si se aplica un MAC con una clave de 256 bits de longitud para proteger su integridad. Las credenciales utilizadas para la autorización pueden revelarse durante su transmisión por TLS entre NF, a menos que se aplique el caso 4 de la cláusula 8.3.1.

8.3.4.2 Entre RPMT

Los atacantes pueden interceptar, alterar e inyectar mensajes transmitidos por la interfaz N32 entre RPMT porque la conexión N32-c depende de la autentificación por certificado en TLS para el establecimiento de claves de sesión y es posible que los atacantes adquieran esas claves utilizando ordenadores cuánticos.

8.3.5 Repercusiones para el plano de gestión

Toda modificación, supresión, inserción o reproducción durante la transferencia de datos entre el gestor y los objetos gestionados es posible, pues TLS con autentificación por certificado se ejecuta en el plano de gestión. Esto plantea una seria amenaza para los sistemas IMT-2020, ya que un atacante puede obtener acceso al sistema de gestión de la red IMT-2020.

9 Algoritmos criptográficos de seguridad cuántica

La informática cuántica introduce un paradigma informático totalmente nuevo, lo que afectará a la seguridad tanto de los algoritmos de clave simétrica (por ejemplo, cifrado de bloques) como de los algoritmos de clave pública (como RSA), aunque la gravedad de las consecuencias no será idéntica en ambos casos.

En [b-Moses] se muestra que la informática cuántica divide efectivamente entre dos el número de bits de seguridad de las claves de cualquier algoritmo de clave simétrica y que los ordenadores cuánticos pueden ejecutar algoritmos (por ejemplo, el de [b-Grover]) y hallar una clave de cifrado simétrico con una clave de N bits en $2^{N/2}$ operaciones. Por consiguiente, si la informática cuántica se convierte en realidad, los algoritmos de clave simétrica podrán protegerse simplemente duplicando el tamaño de la clave. Es evidente que esto tendrá consecuencias en el rendimiento del algoritmo de clave simétrica.

En cuanto a los algoritmos de clave asimétrica, como RSA, DSA, ECC y DH, se cree que las consecuencias de la informática cuántica serán bastante serias. Los ordenadores cuánticos pueden ejecutar algoritmos (por ejemplo, el de [b-Shor 1997]) que vencen todos los sistemas de clave pública más utilizados en un tiempo insignificante. Por ejemplo, un algoritmo cuántico denominado algoritmo de Shor puede revelar una clave RSA en un tiempo polinómico [b-Moses].

Los algoritmos criptográficos de seguridad cuántica deben seleccionarse en función de unos criterios de evaluación (véase en el Apéndice IV el ejemplo de criterios de evaluación de NIST).

9.1 Algoritmos de clave simétrica de seguridad cuántica

Está muy extendida la opinión de que los criptosistemas simétricos básicos, como el cifrado de bloques o las funciones de troceo, son algoritmos de seguridad cuántica [b-CSA], como se muestra en el Apéndice III. En [b-UIT-T X.1197] puede encontrarse una lista de ejemplos de algoritmos de seguridad cuántica con sus longitudes de clave. La aparición de ordenadores cuánticos criptográficamente relevantes exigirá un notable aumento del tamaño de las claves simétricas, equivalente al doble de las actuales claves de 128 bits utilizadas en los sistemas IMT-2020. En [b-CSA] se indica que la longitud de clave actualmente recomendada de 256 bits se considera segura, incluso contra el algoritmo de Grover.

9.2 Algoritmo de clave asimétrica de seguridad cuántica

Aunque los ordenadores cuánticos pueden ejecutar algoritmos que vencen los actuales sistemas de clave pública (por ejemplo, RSA y ECC) en cantidades de tiempo insignificantes, como se muestra en el Apéndice III, hay muchos tipos de sistemas criptográficos superiores a RSA y ECC que son seguros contra un ataque cuántico; esos sistemas se describen en las cláusulas 9.2.1 a 9.2.5. Puede encontrarse una lista de las actuales normas en materia de algoritmos asimétricos de seguridad cuántica en [b-UIT-T X.1197].

NOTA – La distribución de clave cuántica (QKD, *quantum key distribution*) es un método de implementación del acuerdo de claves que ha demostrado ser robusto contra la informática cuántica.

9.2.1 Algoritmos de celosía

Los algoritmos de celosía se basan en problemas difíciles bien conocidos de la celosía para construir primitivas criptográficas de seguridad cuántica. Uno de ellos es el problema de vector más corto (SVP, *shortest vector problem*), es decir, encontrar el vector distinto de cero más corto en una celosía dada, que ha demostrado ser un problema difícil en tiempo polinómico no determinista (NP-hard, *non-deterministic polynomial time-hard*) no determinista para reducciones aleatorizadas [b-Ajtai].

En [b-CSA] se indica que los algoritmos de celosía pueden servir para la firma digital, la encriptación de clave pública o privada y el acuerdo de claves. En la cláusula II.1 se enumeran algunos algoritmos de celosía.

9.2.2 Algoritmos de número generador

Los algoritmos de número generador se basan en la seguridad de la función de troceo criptográfica subyacente.

En [b-CSA] se muestra que los algoritmos de número generador se utilizan para firmas digitales construidas con funciones de troceo. En la cláusula II.2 se enumeran algunos algoritmos de número generador.

9.2.3 Algoritmos de código

Los algoritmos de código dependen de algunos códigos de corrección de errores, cuyos esquemas de codificación son difíciles de descodificar eficazmente incluso para un ordenador cuántico. Por ejemplo, el criptosistema de McEliece [b-McEliece] se basa en el problema NP-hard de descodificación de un código lineal general.

En [b-CSA] se indica que los algoritmos de código pueden servir para firmas digitales, encriptación de clave pública o privada y acuerdo de claves. En la cláusula II.3 se enumeran algunos algoritmos de código.

9.2.4 Algoritmos multivariante

Los algoritmos multivariante se basan en la dificultad de solucionar sistemas de ecuaciones polinomiales multivariante no lineales en campos finitos. Se sabe que este problema es NP-hard [b-Garey].

En [b-CSA] se indica que los algoritmos multivariante pueden servir para firmas digitales y encriptación de clave pública o privada. En la cláusula II.4 se muestran algunos esquemas de firma basados en algoritmos multivariante.

9.2.5 Algoritmos de isogenia de extrema singularidad

Los algoritmos de isogenia de extrema singularidad se construyen sobre la base de la dificultad que supone recuperar una isogenia desconocida entre un par de curvas elípticas de extrema singularidad que se sabe son isógenas.

Ofrecen una seguridad hacia delante perfecta y pueden servir de sustituto directo y resistente a la informática cuántica de los métodos DH y ECDH. Un ejemplo típico es el algoritmo de isogenia Diffie-Hellman de extrema singularidad (SIDH, *supersingular-isogeny Diffie–Hellman*) [b-Jao].

10 Directrices para la utilización de algoritmos criptográficos de seguridad cuántica en sistemas IMT-2020

En primer lugar se considera en términos generales el tratamiento del notable incremento del tamaño de los mensajes cuando se introduzcan algoritmos asimétricos de seguridad cuántica en los sistemas IMT-2020. Se tiene en consideración posteriormente la utilización de algoritmos criptográficos de seguridad cuántica en IPsec, TLS y DTLS, pues se han desplegado en más de un sitio en los sistemas IMT-2020. Por último se especifican las directrices de aplicación de algoritmos criptográficos de seguridad cuántica a la red de acceso IMT-2020 y la red dorsal IMT-2020.

10.1 Tamaño del mensaje

El tamaño de los mensajes que contiene una clave pública, un texto cifrado o una firma aumentará considerablemente, pues los algoritmos asimétricos de seguridad cuántica suelen ser mucho más grandes que los algoritmos asimétricos clásicos en lo que a claves públicas, textos cifrados o firmas se refiere. Por ejemplo, en los algoritmos asimétricos de seguridad cuántica la clave pública oscila entre 726 bytes y casi 1 Mbyte, como se muestra en la cláusula II.5, mientras que el tamaño de una clave pública en los algoritmos asimétricos clásicos suele oscilar entre 32 bytes y 256 bytes. El Instituto Nacional de Normas y Tecnología (NIST) tiene previsto normalizar más de un algoritmo asimétrico de seguridad cuántica. Se deduce, por tanto, que habrán de escogerse para los sistemas IMT-2020 los algoritmos asimétricos de seguridad cuántica cuyo tamaño de clave pública, texto cifrado o firma sea menor. La norma del sistema IMT-2020 necesita determinar el tamaño de mensaje adecuado para acomodar la clave pública, el texto cifrado o la firma cuando se utilizan algoritmos asimétricos de seguridad cuántica.

10.2 IPsec, TLS y DTLS

Si se aplica PSK a la autentificación y el acuerdo de claves, se recomienda que la PSK sea de 256 bits, y se recomienda utilizar algoritmos simétricos de seguridad cuántica cuya longitud de claves sea de 256 bits para proteger la confidencialidad y la integridad de los mensajes transmitidos por la red. Si se utilizan esquemas de autentificación por certificado, se recomienda integrar algoritmos asimétricos de seguridad cuántica en los protocolos de autentificación a fin de que la autentificación y el acuerdo de claves de sesión tenga seguridad cuántica; y se recomienda utilizar algoritmos simétricos de seguridad cuántica con claves de 256 bits de longitud para la protección de la confidencialidad y la integridad de los mensajes. De este modo, SDN, NDS/IP y el plano de gestión no serán vulnerables a los ataques cuánticos.

El IETF aún no ha empezado a estudiar cómo añadir algoritmos de seguridad cuántica a las series cifradas de IPsec, TLS y DTLS, pues el NIST no ha terminado de definir los posibles algoritmos asimétricos de seguridad cuántica. Se prevé que los proyectos de normas del NIST estén disponibles entre 2022 y 2024 [b-Moody]. Una vez que el IETF haya especificado las series cifradas cuánticamente resistentes para IPsec, TLS y DTLS, habida cuenta del escaso ancho de banda

inalámbrico y de las limitadas capacidades de computación de los dispositivos, se recomendará la utilización en sistemas IMT-2020 de una serie cifrada con un menor tamaño de clave y una encriptación de alta velocidad.

10.3 Capa de infraestructura

Se recomienda que una SDN aplique las sugerencias especificadas en la cláusula 10.2 cuando se utilicen IPsec y TLS.

Se recomienda sustituir los algoritmos criptográficos clásicos utilizados en la capa NFVI por algoritmos criptográficos de seguridad cuántica, tanto de tipo simétrico como asimétrico.

10.4 Red de acceso IMT-2020

10.4.1 Privacidad del abonado

Se recomienda que el esquema ECIES aplique para generar la clave compartida algoritmos asimétricos de seguridad cuántica tipo DH, como la encapsulación de claves de isogenia de extrema singularidad (SIKE, *supersingular isogeny key encapsulation*) y NewHope, han pasado a la segunda ronda del procedimiento de normalización de la criptografía postcuántica (PQC, *post-quantum cryptography*) del NIST (véase el Apéndice II). Se recomienda ocultar el SUCI con un algoritmo simétrico de seguridad cuántica con una clave compartida de 256 bits.

10.4.2 Autentificación

Dado que la serie de algoritmos MILENAGE soporta sólo claves de 128 bits, mientras que la serie de algoritmos TUAK soporta claves de 256 bits, se recomienda utilizar la serie de algoritmos TUAK, en lugar de MILENAGE, en el procedimiento de autentificación para generar el AV y la respuesta de autentificación.

10.4.3 Jerarquía de claves

Para generar la clave de sesión K_{SEAF} con una entropía de 256 bits, la jerarquía de claves debe proceder a las siguientes adaptaciones: (1) se recomienda que la clave raíz K tenga un tamaño de 256 bits; (2) se recomienda no truncar los resultados de 256 bits de la GKDF.

En la práctica, la longitud de la clave raíz K suele ser de 128 bits, dado que en los sistemas IMT-2020 se utilizan tarjetas USIM heredadas con esa configuración. Las nuevas tarjetas USIM utilizadas para los primeros sistemas IMT-2020 por muchos operadores almacenarán sólo una clave raíz de 128 bits. Por consiguiente, la entropía de la clave de sesión K_{SEAF} derivada de la clave K sólo será de 128 bits, lo que no ofrece seguridad cuántica.

Para aumentar la seguridad de la clave de sesión K_{SEAF} actual cuando la tarjeta USIM tenga una clave de 128 bits, la generación de la clave de sesión K_{SEAF} actual se basa no sólo en la primera clave de sesión K_{SEAF}`, determinada por la clave K a largo plazo, sino también en al menos una de las claves adicionales. Las claves adicionales pueden ser la clave de sesión inicial $K_{SEAF\_INITIAL}$ generada la primera vez que el EU se conecta a la red y/o la clave de sesión K_{SEAF_PRV} utilizada en la sesión anterior. Tanto la primera clave de sesión como las claves adicionales son claves simétricas, lo que significa que tanto el EU como la red las comparten. De este modo, la entropía de la clave de sesión K_{SEAF} actual será como mínimo de 256 bits, pues la entropía de la primera clave de sesión K_{SEAF}` es de 128 bits y la entropía de las claves adicionales (clave $K_{SEAF\_INITIAL}$ y/o clave K_{SEAF_PRV}) es, como mínimo, de 128 bits.

Una buena práctica consiste en poder utilizar nuevas tarjetas SIM para lograr una entropía de 256 bits para la clave de sesión K_{SEAF}. Puede tratarse de SIM, USIM, eSIM u otros factores y tipos de SIM no normalizados con las adaptaciones correspondientes para:

a) el almacenamiento de una clave raíz de 256 bits para el mismo fin que la clave raíz K en las antiguas (U)SIM;

b) el soporte de una aceleración del *hardware* para los necesarios KDF y bucle de núcleo criptográfico simétrico (por ejemplo, AES) en las nuevas tarjetas SIM. Esto es particularmente importante para la IoT y en los países donde los teléfonos básicos representan una proporción notable del número total de dispositivos celulares en uso, si bien pueden compatibilizarse con una IMT-2020 de seguridad cuántica –aunque no rápida– mediante la reutilización de frecuencias y la traducción de protocolos.

10.4.4 Seguridad de la señalización NAS, la señalización AS y los datos de usuario

Como se indica en la cláusula 7, los algoritmos de clave simétrica de 128 bits, como AES-128, SNOW 3G y ZUC-128, son la base de la protección de la confidencialidad y la integridad de la señalización NAS, la señalización AS y los datos de usuario en una red de acceso IMT-2020.

Para resistir ataques cuánticos, se recomienda utilizar en los sistemas IMT-2020 algoritmos de clave simétrica de 256 bits. Los MAC de mayor tamaño ofrecen una mejor protección contra los ataques que adivinan el MAC correcto del mensaje. En [b-NIST SP 800-38B] se recomienda utilizar un MAC de 64 bits de longitud mínima para la protección contra los ataques por adivinación. La longitud del MAC en una red de acceso IMT-2020 es de apenas 32 bits. Aumentar el tamaño del MAC de 32 a 64 bits tiene grandes consecuencias para la red IMT-2020 y el protocolo. Queda en estudio si una red de acceso IMT-2020 puede defenderse contra ataques por adivinación cuando se aplican algoritmos simétricos de seguridad cuántica de 256 bits para generar un MAC de 32 bits de longitud.

10.4.5 Seguridad del acceso no 3GPP

Véase en la cláusula 10.2 la estrategia para resistir ataques cuánticos al acceso no 3GPP, pues la seguridad del acceso no 3GPP depende de IPsec.

10.5 Red núcleo IMT-2020

10.5.1 Dentro de una RPMT

1) Autentificación

Para resistir ataques cuánticos se recomienda que la autentificación basada en NDS/IP aplique la estrategia expuesta en la cláusula 10.2.

2) Autorización

Se recomienda utilizar en OAuth 2.0 funciones de troceo con clave segura cuántica, como HMAC-SHA-256, así como algoritmos de firma de seguridad cuántica para garantizar la integridad del testigo de acceso. Véase en la cláusula 10.2 la estrategia para la transición a series cifradas de seguridad cuántica en TLS.

Para JWS se recomienda utilizar algoritmos de firma de seguridad cuántica.

10.5.2 Entre RPMT

Se recomienda aplicar el método presentado en la cláusula 10.2 a la N32-c para evitar que un atacante cuántico derive las claves de sesión. Se recomienda utilizar en una interfaz N32 AES-GCM con una clave de 256 bits para garantizar la confidencialidad y la integridad de la comunicación entre RPMT.

Para JWS se recomienda utilizar algoritmos de firma de seguridad cuántica en lugar de ECDSA.

Apéndice I

Presentación del sistema IMT-2020

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se presenta a grandes rasgos un sistema IMT-2020.

I.1 Arquitectura general

El objetivo de un sistema IMT-2020 es ofrecer una amplia gama de servicios con distintos requisitos de calidad de funcionamiento. Los servicios ofrecidos por redes IMT-2020 pueden dividirse en tres categorías, de acuerdo con las especificaciones del 3GPP: 1) eMBB soporta grandes velocidades de datos y una mayor movilidad del usuario que 4G/LTE; 2) mIoT ofrece comunicaciones tipo máquina masivas; 3) URLLC soporta servicios esenciales de misión que exigen una mayor fiabilidad y una menor latencia. Un sistema IMT-2020 debe ser una plataforma flexible que permita novedades comerciales e integre las industrias verticales, como la automoción, la manufactura, la energía, la cibersalud y el entretenimiento. Además, el despliegue y el mantenimiento de los sistemas IMT-2020 serán más fáciles que los de generaciones anteriores de redes móviles. Para afrontar estos exigentes requisitos, los sistemas IMT-2020 introducen una serie de tecnologías innovadoras, como la segmentación de red, la NFV, la SDN, la SBA y la separación unidad central/unidad distribuida (CU/DU).

La arquitectura general de un sistema IMT-2020, ilustrada en la Figura I.1, puede dividirse en capa de infraestructura, capa de red, capa de servicio y plano de gestión, en función de la funcionalidad.

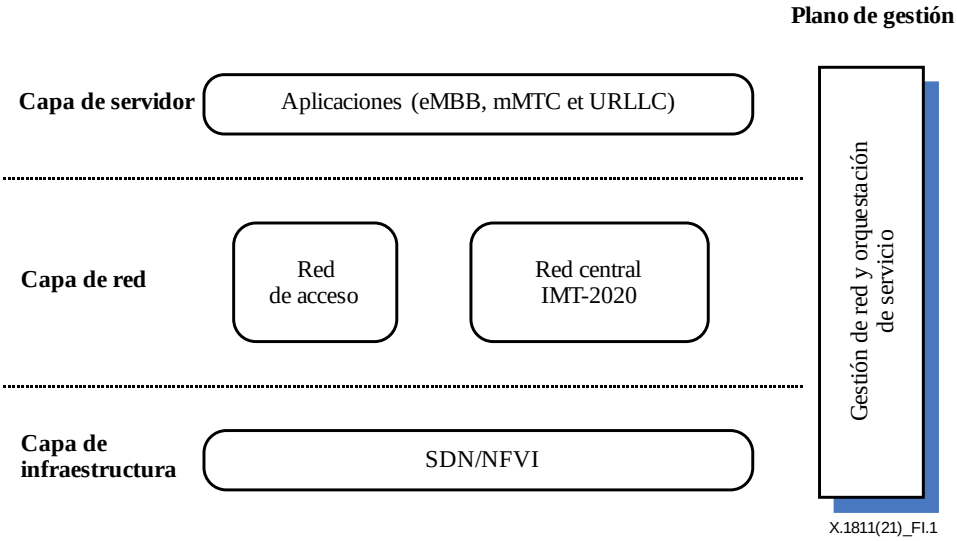

Figura I.1 – Arquitectura general de un sistema IMT-2020

– La capa de infraestructura comprende la SDN y la NFVI. La SDN se utiliza para transportar paquetes a su destino. Además de las tecnologías de transporte heredadas (por ejemplo, conmutación por etiquetas multiprotocolo (MPLS, *multiprotocol label switching*)), los sistemas IMT-2020 introducen la tecnología SDN para lograr una mayor velocidad de transporte y una más fácil adaptación a los requisitos del servicio. La NFVI es la base común para la ejecución de VNF.

– La capa de red se compone de las redes de acceso y núcleo. La primera permite al EU acceder a la red IMT-2020 desde cualquier lugar. La segunda se diseña teniendo en mente una SBA con fines de ampliabilidad y sencillez. Está compuesta de una serie de NF para soportar la conectividad de datos y el despliegue de servicio, por ejemplo, AUSF, AMF y SMF.

– La capa de servicio está formada por las aplicaciones que se ejecutan sobre el sistema IMT-2020, que pueden ser aplicaciones eMBB, aplicaciones de comunicación tipo máquina masiva (mMTC, *massive machine-type communication*) y aplicaciones URLLC.

– El plano de gestión es responsable de la gestión de la red y la orquestación del servicio.

I.2 SDN

El principio básico de la SDN es la disociación del plano de datos del plano de control (CP, *control plane*) a fin de que soporte la programabilidad dinámica de los nodos de red durante el proceso de transmisión de datos. El controlador SDN toma las decisiones de interconexión de redes y envía las normas de transmisión resultantes a los nodos de red. Este mecanismo de transmisión simplifica el reconocimiento de los nodos de red y conduce a una mejor calidad de funcionamiento del plano de datos. En la Figura I.2 se ilustra la arquitectura de la SDN.

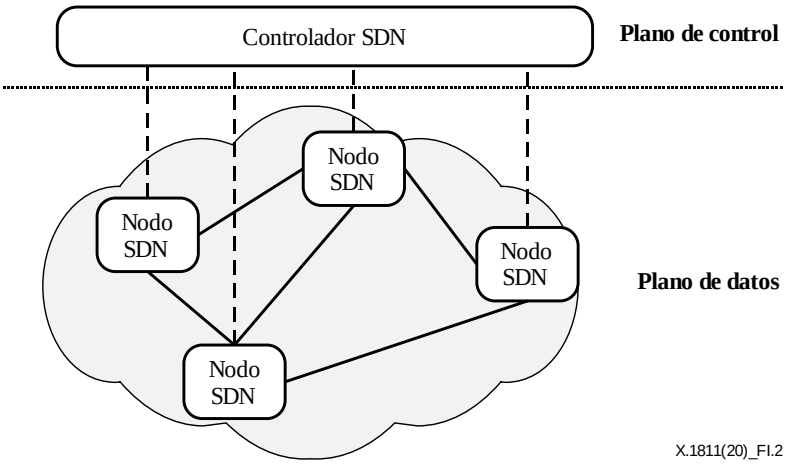

Figura I.2 – Arquitectura de la SDN

I.3 Red de acceso

Un EU puede acceder a una red núcleo IMT-2020 mediante un acceso no 3GPP no fiable o un acceso 3GPP, como se muestra en la Figura I.3. La red de acceso ofrece servicios relacionados con la transmisión de los datos por la interfaz radioeléctrica.

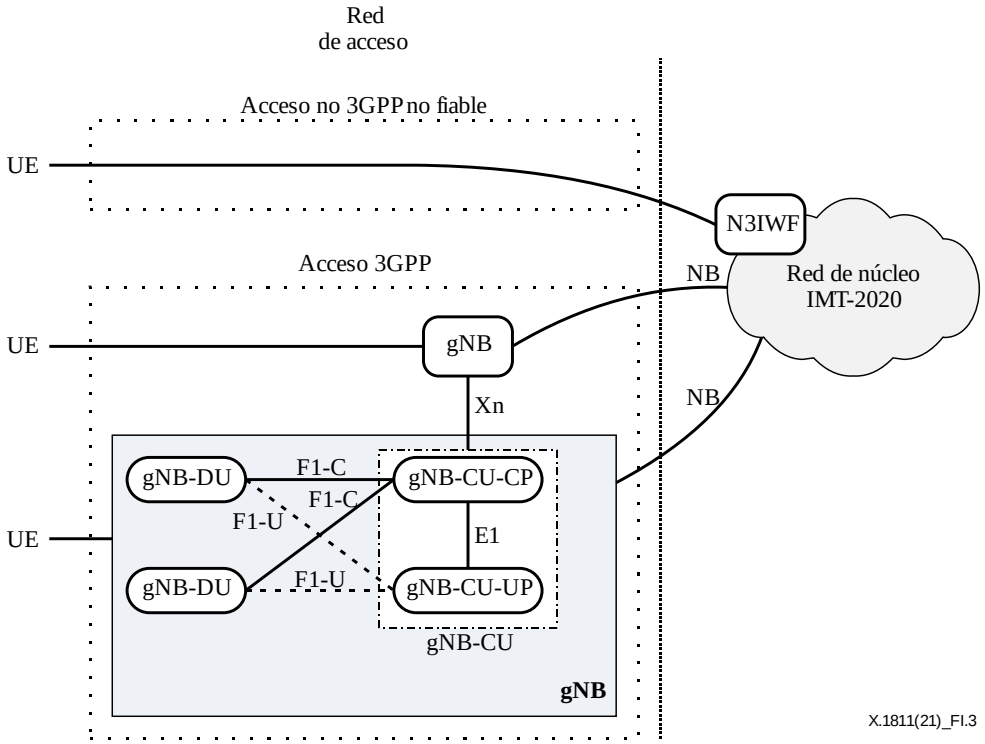

Figura I.3 – Red de acceso

– **Acceso no 3GPP no fiable**

Por acceso no 3GPP no fiable se entiende una tecnología de acceso no especificada por el 3GPP y en la que no confía la red núcleo IMT-2020, como, por ejemplo, el acceso de red de área local inalámbrica (WLAN, *wireless local area network*). En este contexto, el EU se conecta a la red núcleo IMT-2020 a través de una N3IWF.

– **Acceso 3GPP**

El acceso 3GPP es una tecnología de acceso especificada por el 3GPP, es decir, una tecnología de red de acceso radioeléctrico de la próxima generación (NG-RAN, *next generation-radio access network*) en el contexto de la IMT-2020. Un EU puede acceder a la red núcleo IMT-2020 a través de una interfaz NG mediante un gNB plano sin separación CU/DU. Una interfaz NG es una interfaz lógica que soporta el intercambio de información CP e información UP entre el gNB y la red núcleo IMT-2020. Para desplegar la red de manera más flexible y a menor coste, un gNB puede dividirse en gNB-DU y gNB-CU. Un gNB-CU es un nodo lógico que aplica protocolos de capa superior, incluidos el protocolo de adaptación de datos de servicio (SDAP, *service data adaptation protocol*), el control de recursos radioeléctricos (RRC, *radio resource control*) y el protocolo de convergencia de datos en paquetes (PDCP, *packet data convergence protocol*). Un gNB-DU es un nodo lógico que realiza las funciones de capa inferior, incluido el control del enlace radioeléctrico (RLC, *radio link control*), el control de acceso al medio (MAC, *medium access control*) y las funciones de capa física.

Inspirado en la SDN, el gNB-CU puede dividirse además en gNB-CU-CP y gNB-CU-UP, dando como resultado una descomposición funcional del acceso radioeléctrico entre las entidades CP y de usuario. Esta separación del CP y del UP ofrece flexibilidad para operar y gestionar redes complejas, soportar distintas topologías de red, recursos y nuevos requisitos de servicio.

Las unidades gNB-CU y gNB-DU se conectan a través de una interfaz lógica F1, que puede diferenciarse en interfaz F1-C para conectar el gNB-CU-CP e interfaz F1-U para conectar el gNB-CU-UP. Un gNB-CU-CP comunica con un gNB-CU-UP a través de una interfaz E1.

I.4 Red núcleo

La red núcleo IMT-2020 se define como una SBA, tal y como se muestra en la Figura I.4. En la SBA se han definido diversas NF con diversos objetivos. Cada NF ofrece una serie de servicios, denominados servicios NF, que consumen otras NF autorizadas. Las NF recurren a una NRF para descubrirse y comunicarse mutuamente.

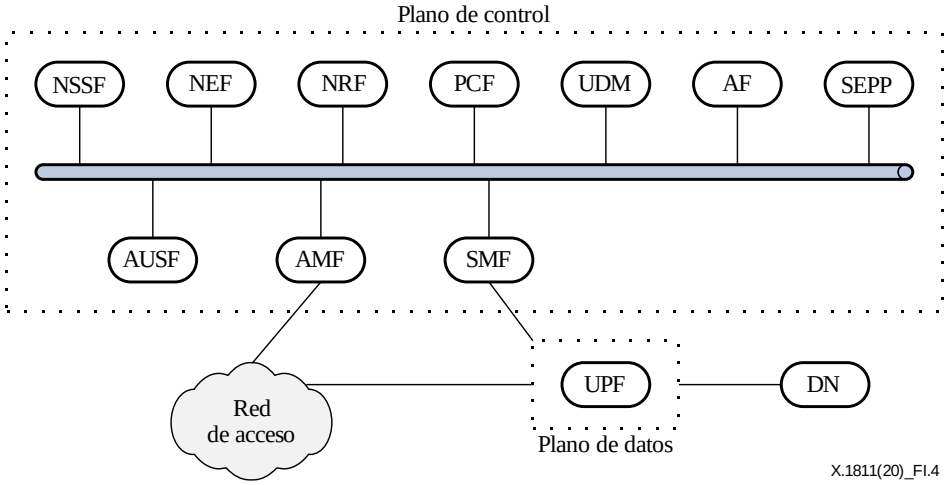

Figura I.4 – Red núcleo IMT-2020

La red núcleo IMT-2020 puede dividirse en CP y UP.

– **Plano de control**

  Este plano ofrece a la red servicios de control, incluido el control del acceso, la movilidad, la política, la exposición, la intercepción legal y la tarificación. En el CP se han definido las siguientes NF:

– **Función selección de segmento de red** (NSSF, *network slice selection function*), que se utiliza para seleccionar el conjunto de segmentos de red que sirven al EU.

– **Función exposición de red** (NEF, *network exposure function*), que soporta la exposición de capacidades y eventos. Las NF exponen capacidades y eventos a otras NF a través de la NEF. Las capacidades y eventos expuestos por una NF pueden exponerse de manera segura a, por ejemplo, terceros, funciones de aplicación y computación periférica.

– **Función repositorio NF** (NRF, *NF repository function*), que se ocupa de las funciones de registro y descubrimiento a fin de que las NF puedan descubrirse y comunicarse entre ellas a través de las API.

– **Función control de política** (PCF, *policy control function*), que soporta un marco político unificado que rige el comportamiento de la red.

– **Gestión de datos unificados** (UDM, *unified data management*), que almacena los datos y perfiles de los abonados. La UDM también se utiliza para generar los AV para AKA 3GPP.

– **Función aplicación** (AF, *application function*), que interactúa con la red núcleo 3GPP para prestar servicios. La AF también ofrece información sobre el flujo de paquetes a la PCF.

– **Intermediario de protección del perímetro de seguridad** (SEPP, *security edge protection proxy*), que es un intermediario no transparente utilizado para proteger los mensajes intercambiados por interfaces CP entre RPMT y ocultar la topología de la red dentro de la RPMT.

– **Función servidor de autentificación** (AUSF, *authentication server function*), que tramita las solicitudes de autentificación tanto para el acceso 3GPP como para el acceso no 3GPP.

– **Función gestión de acceso y movilidad** (AMF, *access and mobility management function*), que se ocupa de la gestión de la autentificación, la autorización y la movilidad de los EU.

– **Función gestión de sesión** (SMF, *session management function*), que se utiliza para gestionar la sesión, por ejemplo, establecimiento, modificación y liberación de sesión. La SMF también atribuye direcciones IP a los EU.

– Plano de usuario

La **función plano de usuario** (UPF, *user plane function*) es la única función definida en el UP. La UPF soporta diversas operaciones y funcionalidades relacionadas con los paquetes UP, como el encaminamiento y la transmisión de paquetes, el manejo del tráfico, la inspección de paquetes y la duplicación de paquetes.

La red núcleo IMT-2020 difiere notablemente de la red núcleo de anteriores generaciones de redes móviles al poseer las siguientes características:

– **SBA**, cuyos servicios operan con una granularidad más fina que la de las redes heredadas y tienen un bajo grado de acoplamiento, lo que permite comercializar nuevos servicios en poco tiempo y ofrece una mayor flexibilidad para actualizar el sistema.

– **Separación del plano de control y el plano de usuario**, que permite desplegar la UPF más cerca del EU a fin de poder cumplir los estrictos requisitos de latencia de los servicios URLLC. La separación del plano de control y el plano de usuario también permite adaptar independientemente los recursos de cada plano.

– **Separación de la AMF y la SMF**, que permite gestionar el acceso y la movilidad de manera centralizada. Por el contrario, la SMF puede ubicarse allí donde los servicios la necesiten.

– **NFV**, donde la red núcleo IMT-2020 supone que las NF se implementan de manera virtualizada para gestionar mejor los recursos y ahorrar costes. Una NFV que separa el *hardware* y el *software* hace que la red sea más flexible y sencilla al minimizar la dependencia de las limitaciones del *hardware*.

– **Segmento de red**, cuyo objetivo es soportar múltiples tipos de servicio en una infraestructura de red física común. Puede ofrecer redes de extremo a extremo personalizadas para ajustarse a los requisitos del caso. Cada segmento de red puede contener varias NF, en función de los requisitos del servicio.

I.5 Plano de gestión

El plano de gestión se encarga de la gestión de la red y la orquestación del servicio. Para gestionar y supervisar las redes, el plano de gestión se conecta a la red de acceso, la red núcleo y la SDN a través de un canal de comunicación individual exclusivo, como se muestra en la Figura I.5. La gestión de red tiene, como mínimo, las siguientes funcionalidades: gestión de fallos (FM, *fault management*), gestión de calidad de funcionamiento (PM, *performance management*), gestión de configuración (CM, *configuration management*) y gestión de rastreo (TM, *trace management*). Aparte de estas funciones de gestión de la red, la gestión de los segmentos de red también necesita de las siguientes funciones: gestión del ciclo de vida del segmento, gestión de la capacidad del segmento y descubrimiento de recursos de red. La orquestación del servicio aplica mecanismos de control y supervisión de recursos flexibles para la configuración, gestión y reoptimización de los servicios de red.

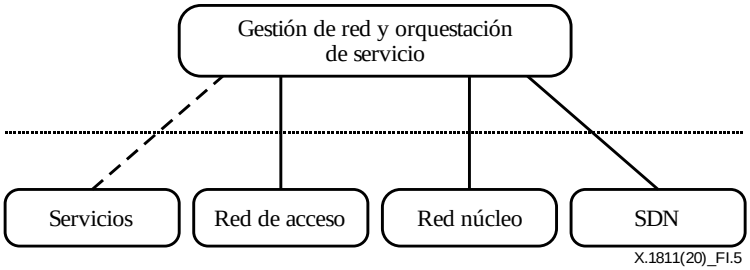

Figura I.5 – Arquitectura de gestión general

Apéndice II

Algoritmos criptográficos de clave asimétrica de seguridad cuántica

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se enumeran los algoritmos criptográficos de clave asimétrica de seguridad cuántica más conocidos.

II.1 Algoritmos de celosía

Entre los algoritmos de celosía se cuentan los siguientes:

– anillo polinomial truncado de enésimo grado (NTRU, *Nth degree truncated polynomial ring*) [b-Hoffstein];

– aprendizaje con errores (LWE, *learning with errors*) [b-Regev];

– aprendizaje con errores en anillo (R-LWE, *ring learning with errors*) [b-Lyubashevsky];

– esquema NewHope [b-Alkim].

II.2 Algoritmos de número generador

Entre los algoritmos de número generador se cuentan los siguientes:

– esquema de firma de Merkle extendido (XMSS, *extended Merkle signature scheme*) [b-Buchmann];

– SPHINCS [b-Bernstein 2015];

– firmas por número generador de Leighton-Micali (LMS, *Leighton-Micali hash-based signatures*) [b-IRTF RFC 8554].

II.3 Algoritmos de código

Entre los algoritmos de código se cuentan los siguientes:

– McEliece clásico [b-McEliece];

– esquema de Niederreiter [b-Dinh].

II.4 Algoritmos multivariante

Entre los esquemas de firma prácticos basados en algoritmos multivariante se cuentan los siguientes:

– Rainbow [b-Ding];

– aceite y vinagre desequilibrados (UOV, *unbalanced oil and vinegar*) [b-Kipnis].

II.5 Normalización de la criptografía postcuántica por el NIST

El 20 de diciembre de 2016, el NIST publicó la petición de candidaturas de algoritmos criptográficos de clave pública postcuánticos. En la primera ronda, el NIST aceptó 69 candidaturas, de las cuales 20 eran esquemas de firma digital y 49 encriptaciones de clave pública (PKE) o mecanismos de encapsulación de claves (KEM). El 30 de enero de 2019, el NIST seleccionó en segunda ronda los 26 algoritmos que se presentan en el Cuadro II.1, nueve de los cuales son esquemas de firma digital y 17 PKE y esquemas de establecimiento de claves [b-NISTIR 8240].

Cuadro II.1 – Algoritmos de la segunda ronda del NIST

Clasificación	Problema base	Algoritmo
Encriptación/KEM	Celosía	Crystals-Kyber
		FrodoKEM
		LAC
		NewHope
		NTRU
		NTRU Prime
		Round 5
		Saber
		Three Bears
	Código	Classic McEliece
		NTS-KEM
		BIKE
		HQC
		Rollo
		LEDAcrypt
		RQC
	Isogenia	SIKE
Firma	Celosía	Crystals-Dilithium
		Falcon
		qTesla
	Multivariante	GeMSS
		LUOV
		MQDSS
		Rainbow
	Número generador	Sphincs+
		Picnic

El NIST tiene la intención de normalizar algoritmos de clave pública postcuánticos para su utilización en una amplia variedad de protocolos, como TLS, intérprete de comandos seguro (SSH, *secure shell*), intercambio de claves Internet (IKE, *Internet key exchange*), IPsec y extensión de seguridad del sistema de nombre de dominio (DNSSEC, *domain name system security extensions*) [b-NISTIR 8240].

El NIST evalúa los algoritmos de segunda ronda desde el punto de vista de la seguridad y de la calidad de funcionamiento. La encriptación NTRU se inventó en 1996 y su seguridad se ha estudiado durante décadas hasta llegar a entenderla razonablemente bien. Además, la encriptación NTRU está normalizada en [b-IEEE Std 1363.1]. McEliece clásico se basa en [b-McEliece], que nunca se ha vencido y se considera seguro en un mundo cuántico. Por el contrario, muchos otros esquemas existen desde unos diez años apenas, por lo que aún es necesario que la comunidad criptográfica los criptoanalice en profundidad para aumentar la confianza en su seguridad. Concretamente, SIKE, cuyo origen es [b-Jao], depende del problema que supone encontrar isogenias entre curvas elípticas de extrema singularidad, problema que no se ha estudiado tanto como los problemas de seguridad asociados a otros candidatos [b-NISTIR 8240].

El secreto perfecto hacia adelante implica que no se revelarán las claves de sesiones anteriores, incluso si se expone la clave a largo plazo. Se trata de una propiedad de seguridad útil que desean los protocolos de seguridad más utilizados, como IPsec y TLS. De todos los candidatos, sólo SIKE y NewHope pueden soportar el secreto perfecto hacia adelante.

El rendimiento de los algoritmos se mide en términos del tamaño de las claves públicas, el texto cifrado y la firmas, así como de la eficacia del cálculo de la encriptación y la desencriptación. Los algoritmos PQC suelen tener claves públicas, textos cifrados y firmas de mucho mayor tamaño que los algoritmos de clave pública clásicos. Las claves públicas de los candidatos oscilan entre 726 bytes y más de 1 Mbyte, de acuerdo con [b-NIST PQC]. SIKE tiene la clave pública de menor tamaño, mientras que la clave pública de McEliece clásico y NTS-KEM es mucho más grande que la de otros esquemas. Sin embargo, McEliece clásico y NTS-KEM pueden generar textos cifrados más pequeños que otros esquemas con una velocidad de encriptación competitiva. El rendimiento de SIKE parece ser un orden de magnitud más lento que el de muchos de los demás candidatos, a pesar de tener la clave pública de menor tamaño. A la hora de seleccionar los algoritmos PQC es, por tanto, necesario llegar a un equilibrio entre eficiencia de ancho de banda y eficiencia del cálculo.

En 2020 NIST tiene previsto seleccionar a los finalistas para una última ronda o seleccionar un pequeño número de candidatos a la normalización [b-NISTIR 8240], lo que implica que no se normalizará sólo uno, sino varios algoritmos PQC. En el entorno móvil, el rendimiento reviste una importancia crítica, dada la escasez de recursos inalámbricos de la interfaz inalámbrica y las limitadas capacidades de cálculo de los dispositivos. Los algoritmos finalmente normalizados, que tendrán las claves públicas y textos cifrados de menor tamaño y una velocidad de encriptación competitiva, se introducirán en los sistemas IMT-2020.

Apéndice III

Repercusiones de la informática cuántica en los algoritmos criptográficos comunes

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se enumeran las repercusiones de la informática cuántica en los algoritmos criptográficos comunes.

En el Cuadro III.1 se resumen las repercusiones de los ordenadores cuánticos a gran escala en los algoritmos criptográficos comunes, como RSA y la norma de encriptación avanzada (AES).

No se sabe hasta qué punto pueden llevarse las ventajas cuánticas, ni qué distancia media entre la viabilidad en el modelo clásico y el modelo cuántico [b-NISTIR 8105].

Cuadro III.1 – Repercusiones de los ordenadores cuánticos en los algoritmos criptográficos más utilizados [b-NISTIR Quantum report]

Algoritmo criptográfico	Tipo	Utilización	Repercusiones
AES	Simétrico	Encriptación	Se necesitan claves de gran tamaño
SHA-2, SHA-3	Número generador	Función de troceo	Se necesita un resultado de gran tamaño
RSA	Clave pública	Firma, transporte de claves	Ya no es seguro
ECDSA, ECDH	Clave pública	Firma, intercambio de claves	Ya no es seguro
DSA	Clave pública	Firma, intercambio de claves	Ya no es seguro

Apéndice IV

Criterios de evaluación de la criptografía de seguridad cuántica

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se presentan los criterios de evaluación del NIST para seleccionar la criptografía de seguridad cuántica.

Los algoritmos criptográficos presentados se evaluarán en función de tres aspectos: seguridad, coste y características del algoritmo y su implementación [b-NIST-Sub].

IV.1 Seguridad

La seguridad que ofrece un esquema criptográfico es el factor más importante de la evaluación. Cada esquema se juzgará en función de los siguientes factores:

Aplicaciones de la criptografía de clave pública: se normalizarán los algoritmos postcuánticos para las normas existentes en materia de firma digital (FIPS 186) y establecimiento de claves (SP 800-56A, SP 800-56B), que se utilizan en un amplio abanico de protocolos de Internet, como TLS, SSH, IKE, IPsec y DNSSEC. Los esquemas se evaluarán en función de la seguridad que ofrezcan en estas aplicaciones durante el proceso de evaluación. Las aplicaciones propuestas se evaluarán en función de su importancia práctica, si ello es necesario para decidir qué algoritmos normalizar.

Definición de seguridad para la encriptación/establecimiento de claves: los algoritmos postcuánticos para la encriptación o el establecimiento de claves deben ser "semánticamente seguros" frente a los ataques criptográficos escogidos *ad hoc*. Esta propiedad suele denominarse seguridad *IND-CCA2* en la literatura académica.

La definición de seguridad anterior debe considerarse una declaración de lo que NIST considerará como ataque pertinente. Los esquemas KEM y de encriptación se evaluarán en función de la medida en que parezcan poseer esa propiedad cuando se utilizan como lo especifica la entidad que los presenta. Esas entidades no necesitan presentar pruebas de la seguridad, aunque se tomarán en consideración si las hubiere.

Para estimar la solidez de seguridad puede suponerse que un atacante tiene acceso a la desencriptación de no más de 2^{64} textos cifrados escogidos, aunque podrán considerarse también ataques con más textos cifrados.

Definición de seguridad para la encriptación de efímeros únicamente/establecimiento de claves: si bien la seguridad de textos cifrados escogidos es necesaria para muchas de las aplicaciones existentes (por ejemplo, los protocolos de intercambio nominal de claves efímeras que permiten el almacenamiento temporal de las claves), es posible implementar un protocolo de intercambio de claves exclusivamente efímeras de manera que sólo se necesite la seguridad pasiva de la primitiva de encriptación o KEM.

Para esas aplicaciones, los algoritmos postcuánticos para la encriptación de efímeros únicamente/establecimiento de claves deben ser semánticamente seguros con respecto a los ataques de texto simple escogidos. Esta propiedad suele denominarse seguridad *IND-CPA* en la literatura académica.

Los esquemas KEM y de encriptación presentados se evaluarán en función de la medida en que parezcan poseer esa propiedad cuando se utilizan como lo especifica la entidad que los presenta. Esas entidades no necesitan presentar pruebas de la seguridad, aunque se tomarán en consideración si las hubiere. Deberá explicarse detalladamente toda vulnerabilidad de seguridad resultante de la reutilización de una clave.

Definición de seguridad para las firmas digitales: los algoritmos postcuánticos para firmas digitales permiten lograr firmas digitales esencialmente infalsificables frente a ataques de mensajes escogidos adaptativos. Esta propiedad suele denominarse *seguridad EUF-CMA* en la literatura académica.

Los algoritmos presentados para firmas digitales se evaluarán en función de la medida en que parezcan poseer esa propiedad cuando se utilizan como lo especifica la entidad que los presenta.

A fin de estimar la solidez de la seguridad, puede suponerse que el atacante tiene acceso a firmas de no más de 2^{64} mensajes escogidos.

Propiedades de seguridad adicionales: si bien las definiciones de seguridad enumeradas anteriormente cubren muchos de los posibles ataques se utilizarán para evaluar los algoritmos presentados, hay varias otras propiedades que convendría tener:

Una de ellas es el secreto perfecto hacia adelante. Aunque esta propiedad puede obtenerse utilizando las funcionalidades de encriptación y firma normalizadas, su coste podría ser prohibitivo en algunos casos. Concretamente, los esquemas de encriptación de clave pública con un algoritmo de generación de claves lento, como RSA, suelen considerarse inadecuados para el secreto perfecto hacia adelante. Se trata de un caso en que el coste y la seguridad práctica de un algoritmo están estrechamente relacionados.

Otro caso en que la seguridad y el rendimiento interactúan es la resistencia a los ataques por canal lateral. Los esquemas que pueden resistir a un ataque por canal lateral con un coste mínimo son más convenientes que aquéllos cuyo rendimiento se ve gravemente menoscabado cuando intentan resistir a ataques por canal lateral. Cabe señalar, además, que las implementaciones optimizadas contra ataques por canal lateral (por ejemplo, implementaciones contantes en el tiempo) son más significativas que las que no prevén esos ataques.

Una tercera propiedad deseable es la resistencia a los ataques multiclave. En una configuración ideal un atacante no debería verse favorecido por atacar múltiples claves al mismo tiempo, sea su objetivo poner en peligro un único par de claves o un gran número de claves.

Por último, una propiedad que convendría tener, aunque esté mal definida, es la resistencia a la utilización indebida. Lo mejor sería que los esquemas no fallasen catastróficamente a causa de errores de codificación aislados, la disfunción de números generadores aleatorios, la reutilización de palabras aleatorias de un solo uso ("nonce"), la reutilización de pares de claves (para la encriptación de efímeros únicamente/establecimiento de claves), etc.

Otros factores considerados: dado que la criptografía de clave pública suele contener una estructura matemática sutil, es muy importante que ésta se entienda bien para poder confiar en la seguridad de un criptosistema. Para evaluarla se tienen en cuenta diversos factores. Siendo todos los demás factores iguales, los esquemas simples suelen entenderse mejor que los complejos. Del mismo modo, los esquemas cuyos principios de diseño pueden relacionarse con un corpus de investigación establecido suelen entenderse mejor que los esquemas completamente nuevos o que se han diseñado parcheando repetidamente esquemas anteriores, vulnerables al criptoanálisis.

Se tendrán en cuenta la claridad de la documentación del esquema y la calidad del análisis facilitado por la entidad que lo presenta. Un análisis claro y detallado contribuirá a la calidad y madurez del análisis que efectúe la comunidad general. Se tendrán en cuenta los argumentos o pruebas de seguridad que se presenten. Si bien las pruebas de seguridad suelen basarse en supuestos no demostrados, con frecuencia pueden descartar ataques comunes o vincular la seguridad de un nuevo esquema a un problema de cálculo más antiguo y mejor estudiado.

IV.2 Coste

El coste de un criptosistema de clave pública puede medirse en función de diversos factores.

Clave pública, texto cifrado y tamaño de la firma: los esquemas se evaluarán de acuerdo con el tamaño de las claves públicas, los textos cifrados y las firmas que producen. Todos estos factores pueden ser relevantes para las aplicaciones con limitaciones de ancho de banda o protocolos Internet con un tamaño de paquetes limitado. La importancia del tamaño de la clave pública puede variar en función de la aplicación. Si las aplicaciones pueden almacenar temporalmente las claves públicas o disponen de otro mecanismo para no tener que transmitirlas frecuentemente, el tamaño de la clave pública puede revestir una importancia menor. Por el contrario, las aplicaciones cuyo objetivo es lograr un secreto perfecto hacia adelante mediante la transmisión de una nueva clave pública al inicio de cada sesión probablemente se vean muy beneficiadas por algoritmos que utilizan claves públicas relativamente pequeñas.

Eficiencia de cálculo de las operaciones de clave pública o privada: los esquemas también se evaluarán en función de la eficiencia de cálculo de las operaciones de clave pública (encriptación, encapsulación y verificación de firma) y de clave privada (desencriptación, desencapsulación y firma). El coste computacional de estas operaciones se evaluará en el *hardware* y en el *software*. Es probable que el coste computacional sea importante para casi todas las operaciones, pero algunas aplicaciones pueden ser más sensibles que otras. Por ejemplo, las operaciones de firma y desencriptación pueden realizarse con dispositivos con capacidades de cálculo limitadas, como una tarjeta inteligente. Por el contrario, un servidor que asuma un gran volumen de tráfico podrá tener que invertir una parte consecuente de sus recursos de cálculo en verificar las firmas de cliente.

Eficiencia de cálculo de la generación de claves: los esquemas también se evaluarán en función de la eficiencia de cálculo de sus operaciones de generación de claves, cuando proceda. El caso más habitual en que el tiempo de generación de claves es importante es cuando un algoritmo de encriptación de clave pública o un KEM se utilizan para lograr el secreto perfecto hacia adelante. Sin embargo, es posible que el tiempo de generación de claves también resulte importante para esquemas de firma digital de algunas aplicaciones.

Fallos de desencriptación: algunos algoritmos de encriptación de clave pública y KEM, aun correctamente implementados, producirán en ocasiones textos cifrados que no puedan desencriptarse/desencapsularse. Para la mayoría de aplicaciones es importante que esos fallos de desencriptación sean escasos o nulos. En el caso de los algoritmos con fallos de desencriptación/desencapsulación, las entidades que los presentan deben facilitar la tasa de fallos, así como un análisis de las repercusiones para la seguridad que esos fallos pueden ocasionar. Si bien las aplicaciones siempre pueden obtener una tasa de fallos de desencriptación aceptablemente baja encriptando el mismo texto simple múltiples veces, y los protocolos interactivos pueden simplemente reiniciarse cuando falla el establecimiento de claves, esas soluciones tienen su propio coste en términos de rendimiento.

IV.3 Características de los algoritmos y su implementación

Flexibilidad: Suponiendo una seguridad y un rendimiento globalmente buenos, los esquemas con mayor flexibilidad se adaptarán a las necesidades de más usuarios que los esquemas menos flexibles, por lo que serán preferibles.

Como ejemplos de "flexibilidad" pueden citarse, entre otros, los siguientes:

1) El esquema puede modificarse para ofrecer funcionalidades adicionales que superan los requisitos mínimos de la encriptación de clave pública, el KEM (mecanismo de encapsulación de claves) o la firma digital (por ejemplo, asincronía o intercambio de claves implícitamente autentificadas, etc.).
2) Resulta fácil personalizar los parámetros del esquema para ajustarse a una serie de objetivos de seguridad y metas de rendimiento.
3) Los algoritmos pueden implementarse de manera segura y eficiente en un amplio abanico de plataformas, incluidos los entornos restringidos, como las tarjetas inteligentes.

4) Pueden implementarse algoritmos en paralelo para lograr un mayor rendimiento.

5) El esquema puede integrarse en protocolos y aplicaciones existentes con un número mínimo de modificaciones.

Sencillez: el esquema se juzgará en función de la sencillez relativa de su diseño.

Adopción: en el proceso de evaluación se tendrán en cuenta los factores que puedan dificultar o facilitar la amplia adopción de un algoritmo o implementación, entre otros la cobertura de propiedad intelectual de un algoritmo o implementación y la disponibilidad en términos de licencias concedidas a las partes interesadas. Se tendrán en cuenta las garantías formuladas en las declaraciones de la entidad que presenta los algoritmos y de los detentores de las patentes, con una marcada preferencia por las declaraciones en las que se formulen compromisos para conceder licencias sin compensación, sujetas a términos y condiciones razonables y explícitamente exentas de discriminación injusta.

Bibliografía

[b-UIT-T X.1196] Recomendación UIT-T X.1196 (2012), *Marco para el servicio de descargas y sistemas de protección de contenido en el contexto de la televisión móvil por el protocolo Internet*.

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

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autenticación de entidad*.

[b-UIT-T Y.2014] Recomendación UIT-T Y.2014 (2008), *Funciones de control de conexión de red en las redes de próxima generación*.

[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, versión 16.1.0 (2019), *System architecture for the 5G system*.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[b-Ajtai] Ajtai, M. (1998). The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). En Vitter, J. (editor). *STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, págs. 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 [consultado el 03/02/2020] en 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. En Avanzi, R., Heys H. (editores). *Selected areas in cryptography, SAC 2016*, St. Johns, Canadá, 2016, págs. 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 [consultado el 02/02/2020] en https://www.nature.com/articles/npjqi201619#ref-link-section-82.

[b-Bertoni] Bertoni, G., Daemen, J., Peeters, M., Van Assche, G. "Keccak sponge function family main document". Disponible en 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? En Workshop Record of SHARCS '09: Special-purpose Hardware for Attacking Cryptographic Systems. Disponible [consultado el 03/02/2020] en 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. En Oswald, E., Fischlin, M. (editores). *Advances in Cryptology – EUROCRYPT 2015*, págs. 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. En Yang, B.-Y. (editor). *Post-quantum cryptography*, págs. 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 [consultado el 03/02/2020] en 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. En Rogaway, P. (editor). *Advances in cryptology – CRYPTO 2011*, págs. 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. En Ioannidis, J., Keromytis, A., Yung, M. (editores). *Applied Cryptography and Network Security, ACNS 2005*, págs. 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 [consultado el 02/02/2020] en 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 págs.

[b-Grassl] Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. (2016). Applying Grover's algorithm to AES: Quantum resource estimates. En Takagi T. (editor). *Post-quantum cryptography – PQCrypto 2016*, págs. 29-43. *Lecture Notes in Computer Science*, volume 9606. Cham: Springer. Disponible [consultado el 03/02/2020] en 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. En *STOC '96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, págs. 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. En Yang, B-Y. (editor). *Post-quantum cryptography*, págs. 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. En Stern, J. (editor). *Advances in Cryptology – EUROCRYPT '99*. págs. 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*. En *DSN Progress Report*, No. 44, págs. 114-116. Bibcode:1978DSNPR. Disponible [consultado el 03/02/2020] en 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 págs. Disponible [consultado el 03/02/2020] en 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 págs. Disponible [consultado el 03/02/2020] en 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 págs. 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 [consultado el 03/02/2020] en 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 [consultado el 14/02/2020] en https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

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

[b-NISTIR 8240] National Institute of Standards and Technology Internal Report 8240 (2019), *Status* report on the first round of *the NIST* post-quantum cryptography standardization process. Gaithersberg, MA: National Institute of Standards and Technology. 27 págs. DOI: 10.6028/NIST.IR.8240. Disponible [consultado el 03/02/2020] en 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 [consultado el 14/02/2020] en 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 págs. DOI: 10.6028/NIST.SP.800-38B. Disponible [consultado el 03/02/2020] en 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*. Disponible [consultado el 20-03-2020] en : 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 [consultado el 02/02/2020] en 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 en https://www.engadget.com/2017/11/10/ibm-50-qubit-quantum-computer/.

[b-QC2] Practical Quantum Computers, disponible en 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. En *STOC'05 Proceedings of the 37th Annual ACM Symposium on Theory of Computing*. págs. 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. En Takagi T., Peyrin T. (editores). *Advances in Cryptology – ASIACRYPT 2017*, págs. 241-270. *Lecture Notes in Computer Science*, volume 10625. Cham: Springer. DOI: 10.1007/978-3-319-70697-9_9. Disponible [consultado el 02/02/2020] en 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), págs. 38-40. Disponible [consultado el 03/02/2020] en 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), págs. 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), págs. 303-332. DOI: 10.1137/S0036144598347011.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021