国　际　电　信　联　盟

ITU-T X.1811

(04/2021)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

IMT-2020安全

在IMT-2020系统中应用量子安全算法的安全导则

ITU-T X.1811 建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
IMT-2020安全	**X.1800–X.1819**

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1811 建议书

在IMT-2020系统中应用量子安全算法的安全导则

概要

ITU-T X.1811建议书通过评估当前使用的加密算法的安全强度，确定量子计算对国际移动通信-2020（IMT-2020）系统带来的威胁。本建议书简要回顾了量子安全算法（包括对称和非对称类型），并提供了在IMT-2020系统中应用量子安全算法的导则。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1811	2021-04-30	17	11.1002/1000/14454

关键词

5G系统、非对称算法、IMT-2020系统、量子计算机、量子安全算法、对称算法。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2021

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

引言

国际移动通信-2020（IMT-2020）系统具有支持有不同性能要求的广泛服务的巨大潜力，以形成完全互连社会。为了实现这一具有挑战性的目标，已为 IMT-2020 系统开发了许多创新技术，如网络切片、软件定义网络、虚拟化网络功能和中央单元/分布式单元（CU/DU）分离。安全措施是确保 IMT-2020 系统正常运行的基础。除了使用对称密码算法，IMT-2020 系统中还部署了非对称密码算法。

大规模量子计算机对当前广泛使用的对称和非对称密码算法提出了安全问题。后者在量子计算时代不再提供安全性。此外，对称密码算法必须将密钥长度加倍，以抵御量子计算攻击。为此，在 IMT-2020 系统中部署量子安全密码算法是非常可取的。

本建议书对 IMT-2020 系统及其安全架构进行简要概述、评估量子计算机对 IMT-2020 系统的威胁并简要回顾量子安全算法，但本建议书未对其详细予以说明。安全导则将被包含在一高层建议书中，以使量子安全算法适应 IMT-2020 系统。本建议书旨在为量子安全对称和非对称算法在 IMT-2020 系统中的应用以及量子安全对称和非对称算法之间安全级别的统一提供导则。

ITU-T X.1811 建议书

在IMT-2020系统中应用量子安全算法的安全导则

1 范围

本建议书涵盖：

– 国际移动通信-2020（IMT-2020）系统安全架构介绍；

– 当商用量子计算机可用时，对IMT-2020系统的安全评估；

– IMT-2020系统中量子安全算法使用的规范。

2 参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的 ITU-T 建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T X.800] ITU-T X.800建议书（1991），CCITT应用的开放系统互连（OSI）安全体系结构。

[ITU-T X.1038] ITU-T X.1038建议书（2016），软件定义网络的安全要求和参考体系结构。

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 认证 authentication [b-ITU-T Y.2014]：以需要的把握确定实体或当事人的正确身份的特性。被认证方可以是用户、客户、本地环境或服务网络。

3.1.2 认证协议 authentication protocol [b-ITU-T X.1254]：在实体与验证方之间一个确定的消息序列，可供验证方用来认证一个实体。

3.1.3 授权 authorization [b-ISO 7498-2]：权限的授予，包括基于访问权限授予访问权。

3.1.4 可用性 availability [ITU-T X.800]：已授权实体一旦需要就可访问和使用的特性。

3.1.5 证书 credential [b-ITU-T X.1252]：证明声称之身份和/或权利的一组数据。

3.1.6 保密性 confidentiality [ITU-T X.800]：使信息不泄漏给未授权的个人、实体或过程或者不使信息为其利用的特性。

3.1.7 数据完整性data integrity [ITU-T X.800]：数据未被以未授权方式修改或破坏的特性。

3.1.8 隐私 privacy [ITU-T X.800]：每个人都享有的、控制或影响与其相关的什么信息可被收集和存储以及这些信息可被什么人或对什么人泄露的权利。

3.1.9 密钥层次结构 key hierarchy [b-ITU X.1196]：表示不同密钥之间关系的树结构。在密钥层次结构中，节点代表一个密钥，用于推导由推导节点代表的密钥。一个密钥只能有一个先例，但可以有多个推导节点。

3.1.10 网络功能虚拟化 network function virtualization；NFV [b-ISO/IEC TR 22417]：一种技术，支持在共享物理网络上创建逻辑隔离的网络分区，以便多个虚拟网络的异构集合可在共享网络上同时共存。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

4G	第四代
AES	高级加密标准
AES-CBC	高级加密标准-密码块链接
AES-GCM	高级加密标准-伽罗瓦计数器模式
AES-GMAC	高级加密标准-伽罗瓦消息认证码
AF	应用功能
AKA	认证和密钥协议
AMF	访问和移动管理功能
API	应用编程接口
ARPF	认证证书存储库和处理功能
AS	接入层
AUSF	认证服务器功能
AV	认证矢量
CEK	内容加密密钥
CM	配置管理
CP	控制平面
CU/DU	中央单元/分布式单元
DH	迪菲-赫尔曼（Diffie-Hellman）
DHE	迪菲-赫尔曼临时密值（Diffie-Hellman Ephemeral）
DNSSec	域名系统安全扩展
DSA	数字签名算法
DTLS	数据报传送层安全性
EAP	可扩展认证协议
ECC	椭圆曲线密码术

ECDH	椭圆曲线迪菲-赫尔曼
ECDHE	椭圆曲线迪菲-赫尔曼临时密值
ECDLP	椭圆曲线离散对数问题
ECDSA	椭圆曲线数字签名算法
ECIES	椭圆曲线集成加密方案
ECP	扩展切割平面
eMBB	增强移动宽带
ESP	封装安全有效载荷
FM	故障管理
GKDF	通用密钥推导函数
gNB	NR 节点 B
GUTI	全球唯一临时标识符
HMAC	基于散列的消息认证码
HKDF	基于 HMAC 的提取和扩展密钥推导函数
ICV	完整性检验值
IPsec	互联网协议安全性
IKE	互联网密钥交换
IKEv2	互联网密钥交换版本 2
IMT-2020	国际移动通信-2020
IP	互联网协议
IPX	IP 交换
JOSE	Javascript 对象签名和加密
JSON	JavaScript 对象表示法
JWE	JSON 网络加密
JWS	JSON 网络签名
KDF	密钥推导函数
KEM	密钥封装机制
LTE	长期演进
LWE	带错学习
MAC	消息认证码
mIoT	海量物联网
mMTC	海量机器类型通信
MNO	移动网络运营商
MODP	模块化指数
MPLS	多协议标签交换
N3IWF	非 3GPP 互通功能
NAS	非接入层

NDS 网络域安全性
NEF 网络暴露功能
NF 网络功能
NFV 网络功能虚拟化
NFVI 网络功能虚拟化基础设施
NG-RAN 下一代无线接入网
NP 不确定多项式时间
NRF NF 存储库功能
NSSF 网络切片选择功能
NTRU n 次截断多项式环
PCF 政策控制功能
PDCP 分组数据融合协议
PKI 公共密钥基础设施
PKE 公共密钥加密
PM 性能管理
PRF 伪随机函数
PSK 预共享密钥
RLC 无线电链路控制
R-LWE 带错环形学习
RRC 无线电资源控制
RSA 莱维斯特、沙米尔和阿德尔曼（Rivest, Shamir and Adelman）
PLMN 公众陆地移动网络
PQC 后量子密码术
SBA 基于服务的架构
SDAP 服务数据适配协议
SDN 软件定义网络
SEAF 安全地锚功能
SEPP 安全边缘保护代理
SHA 安全散列算法
SIDF 订购标识符去隐藏功能
SIDH 超奇异同源 Diffie–Hellman
SIKE 超奇异同源密钥封装
SMF 会话管理功能
SSH 安全壳
SUCI 订购隐藏标识符
SUPI 订购永久标识符
SVP 最短矢量问题

TLS 传输层安全性
TM 踪迹管理
UDM 统一数据管理
UDR 用户数据存储库
UE 用户设备
UOV 油醋失衡
UP 用户平面
UPF 用户平面功能
URLLC 超可靠和低时延通信
USIM 通用用户识别模块
VNF 虚拟网络功能
WLAN 无线局域网
XMSS 扩展的默克签名方案

5 惯例

本建议书中：

关键词**“要求”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词**“建议”**表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键词**“禁止”**表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键词**“作为选择可以”**表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，厂商可以作为选择提供这一功能，同时仍然声称遵守本建议书提出的规范。

6 概述

IMT-2020 移动通信技术旨在满足 2020 年及未来的业务需求。安全架构是 IMT-2020 网络正常运行的关键。在第四代/长期演进（4G/LTE）技术中，仅使用对称算法来保护信令和用户数据。除此之外，IMT-2020 系统引入了非对称算法，不仅保护用户标识符，还保护移动网络运营商（MNO）之间的通信。

最近（截至 2020 年 9 月），IBM 公布了 50 量子位（qubit）量子计算机[b-QC1]。这一突破打消了最初对大规模量子计算机将在 20 年后上市的预期。目前[b-QC2]新报告估计，这类计算机在 10 年内上市是较为现实的预测。

公钥密码算法的安全性取决于计算问题的难度，如整数分解或不同组上的离散对数问题。现已表明，量子计算机可有效地解决所有这些问题[b-Shor 1997]，从而使一切基于这些假设的公共钥密码系统失效。因此，一台足够强大的量子计算机将危及许多形式的现代密码系统，如密钥交换、加密和数字认证。

量子计算机会对对称和非对称算法的安全强度产生不同程度的影响。对称加密强度将减半，例如，具有 128 位密钥的高级加密标准（AES）提供的 128 位强度将减少到 64 位，而许多常用的非对称算法，如 Rivest、Shamir 和 Adelman（RSA）、数字签名算法（DSA）和椭圆曲线密码术（ECC），将不再提供安全性。

IMT-2020 系统旨在提供具有不同性能要求的广泛服务。IMT-2020 网络提供的服务可分为增强移动宽带（eMBB）、海量物联网（mIoT）和超可靠低时延通信（URLLC）。

IMT-2020 系统引入了许多创新技术，如网络切片、网络功能虚拟化（NFV）、软件定义网络（SDN）和基于服务的架构（SBA）。这些技术使 IMT-2020 系统成为一个灵活的平台，支持新的业务案例并将垂直行业综合一起。另一方面，这些技术使 IMT-2020 系统的安全架构比前几代移动网络复杂得多。

人们迫切希望研究如何通过使用量子安全算法来保护 IMT-2020 系统中的通信，这是因为商业量子计算机很可能在 IMT-2020 系统的寿命周期内变得可用。目前，为 IMT-2020 系统确定的对称算法密钥长度为 128 位。第三代合作伙伴项目（3GPP）刚刚启动了一个研究项目，研究如何将 256 位密钥长度对称算法应用于 IMT-2020 系统[b-3GPP TR 33.841]。然而，迄今为止，还没有研究如何将量子安全的非对称算法应用于 IMT-2020 系统的组织。在 IMT-2020 系统中使用量子安全密码算法时，必须进行一些调整，因为它们的密钥长度比传统密码算法长。此外，有必要研究不同规模的密钥如何在 IMT-2020 系统中共存，因为不可能一夜之间用量子安全算法取代所有传统算法。应尽早考虑在 IMT-2020 系统中向量子安全密码术过渡，这样今后被量子密码分析破坏的任何信息都将不再敏感。

本建议书评估量子计算机对 IMT-2020 系统的威胁，并简要介绍量子安全算法，但本建议书未说明其相关详细。安全导则在高层建议书 – 对量子安全算法加以调整以应用于 IMT-2020 系统 – 中规定。本建议书为量子安全对称和非对称算法在 IMT-2020 系统中的应用以及量子安全对称和非对称算法之间的安全级别统一提供全面的导则。

7 IMT-2020系统安全成份介绍

本节为 ITU-T、3GPP、ETSI、IETF 等已规定的 IMT-2020 系统安全成份提供背景信息。

通信系统应能够提供以下一些安全服务，以确保系统或数据传输的安全[ITU-T X.800]：访问控制（授权）；认证；隐私；保密性；数据完整性；不可否认性；可用性。

安全服务可通过使用密码或非密码机制来实现。本建议书侧重于前者，因为前者研究量子密码算法在 IMT-2020 系统中的应用。

根据附录 I 中介绍的 IMT-2020 系统架构，IMT-2020 系统的安全架构可分为三层：基础设施层、网络层和管理层。

7.1 基础设施层安全性

基础设施层是支持 IMT-2020 系统上层的公共基础，包括 SDN 和网络功能虚拟化基础设施（NFVI）层。

7.1.1 SDN安全性

SDN 技术因其对流量的动态和灵活管理而用于 IMT-2020 中的数据交付。SDN 的安全架构在[ITU-T X.1038]中规定，图 1 对此予以简单说明。

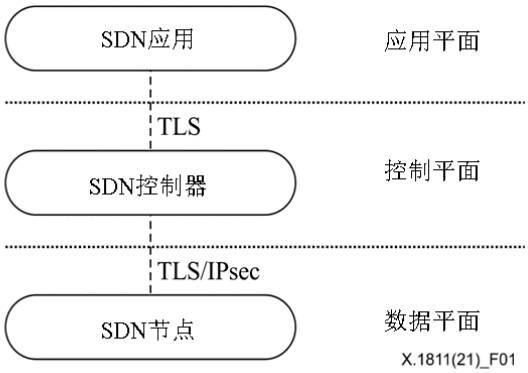


图1 – SDN的安全架构

[ITU-T X.1038]提出了以下与密码算法和协议相关的建议。

建议将传输层安全（TLS）[b-IETF RFC 5246]协议部署在 SDN 应用和 SDN 控制器之间的接口上。基于 TLS，SDN 应用和 SDN 控制器相互认证并就会话密钥达成一致；此外，还确保了应用控制接口上的数据保密性和数据完整性。

建议在 SDN 控制器和 SDN 节点之间的接口上部署 TLS [b-IETF RFC 5246]协议或互联网协议安全（IPSec）协议（[b-IETF RFC 4301]、[b-IETF RFC 4303]、[b-IETF RFC 4835]）。基于 TLS 或 IPsec，SDN 节点和 SDN 控制器相互认证并就会话密钥达成一致；此外，还确保了控制节点接口上的数据保密性和数据完整性。

认证机制可以基于预共享密钥（PSK）[b-IETF RFC 4279][b-IETF RFC 4306]或证书[b-IETF RFC 4306]和[b-IETF RFC 5246]。无论是 RSA [b-ONF TR-511]还是数字签名算法都可应用于基于证书的认证。Diffie-Hellman（DH）或椭圆曲线 Diffie-Hellman（ECDH）密钥交换协议可在 TLS 或 IPsec 环境中实现，以在两个实体之间就共享密钥达成一致。

用于数据加密的密码算法可以是 AES [b-NIST FIPS 197]、河豚（Blowfish）[b-Schneier]或 3DES [b-NIST SP 800-67]。用于数据完整性机制的密码算法可以是消息认证码（MAC）[b-IETF RFC 2104]、基于散列的消息认证码（HMAC）[b-IETF RFC 2104]或数字签名[b-NIST FIPS 186-4]。

7.1.2 NFVI层安全性

NFVI 层支持虚拟网络功能（VNF）的运行，其结构如图 2 所示。

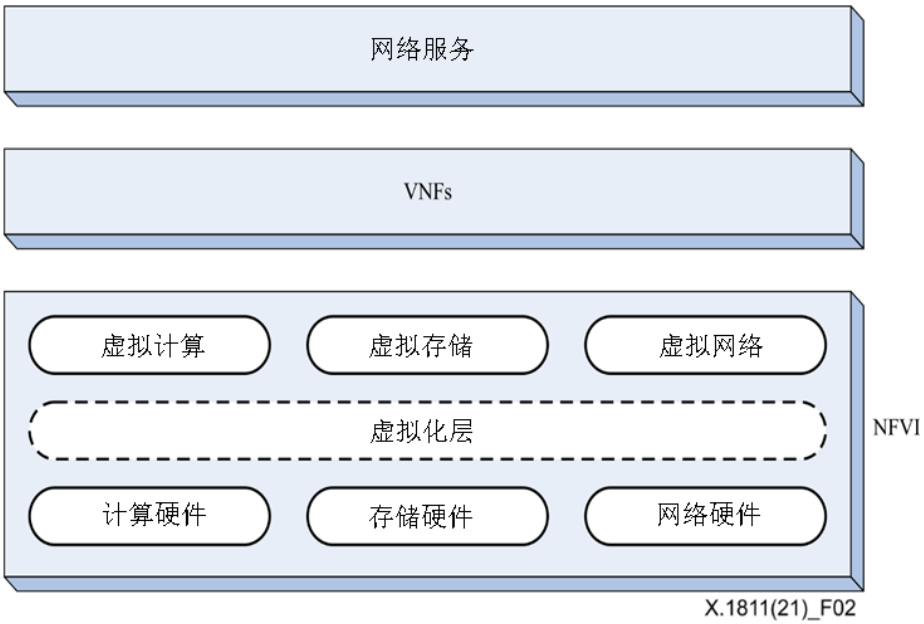


图2 – NFVI结构（改编自[b-ETSI GS NFV 002]图1）

根据[b-ETSI GS NFV-SEC 012]，NFVI 须支持以下安全功能，以确保在其之上运行的VNF的安全性：安全日志记录；操作系统级访问和限制控制；物理控制和警报；认证控制；访问控制；通信安全；证明；硬件调停的执行飞地（enclaves）；基于硬件的信任根；自加密存储；直接访问内存；硬件安全模块；软件完整性保护和验证。为此，NFVI 须实施以下加密算法[b-ETSI GS NFV-SEC 012]：

1) 散列算法：SHA-256、SHA-384、AES128-GMAC、HMAC-SHA128、HMAC-SHA256、HMAC-SHA384；
2) 加密算法：AES-CBC-128、AES-GCM-128（16个八位字节完整性检验值（ICV），AES-CBC-256、AES-GCM-256（16个八位字节ICV）；
3) 签名：RSA 2048、RSA 3072、RSA 4096、ECDSA-256（secp256r1）、ECDSA-384（secp384r1）；
4) 公共密钥基础设施（PKI）：RSA 2048、RSA 3072、RSA 4096、id-ecPublicKey（secp256r1）；
5) 密钥交换：DH组14（2 048位模块化指数（MODP））、DH组19（256位随机扩展切割平面（ECP）组）、DH组20（384位随机ECP组）、椭圆曲线Diffie-Hellman临时密值（ECDHE）secp256r1（P-256）、至少2 048位的Diffie-Hellman临时密值（DHE）组；
6) 伪随机函数（PRF）：PRF-HMAC-SHA2-256、PRF-HMAC-SHA2-384。

7.2 网络层安全性

7.2.1 接入网安全性

接入网络安全性[b-3GPP TS 33.501]旨在确保经过认证的用户设备（UE）能够接入IMT-2020网络，并根据MNO安全政策，可以以可选择的方式保护UE和IMT-2020网络之间的通信。

IMT-2020接入网络的安全架构如图3所示，具体如下。在调用认证和密钥商定（AKA）协议之前，UE 试图使用临时分配的身份或隐藏的永久身份访问网络。UE 和网络通过运行 AKA 协议来相互认证和商定会话密钥。UE 和网络基于会话密钥导出一组密钥。基于这些密钥，在 UE 和接入与移动性管理功能（AMF）之间交换的非接入层（NAS）信令消息的完整性和回复保护是强制性的，而它们的保密性保护是可选的；UE 和 NR 节点 B（gNB）之间交换的接入层（AS）信令消息的完整性和回复保护是强制性的，而它们的保密性保护是可选的。UE 和 gNB 之间的用户平面中的用户数据保密性和完整性保护是可选的。在非 3GPP 接入的情况下，通过使用 IPsec 隧道来保护 UE 和非 3GPP 互通功能（N3IWF）之间的通信。由于 gNB-DU 和 gNB-CU 可以部署在不同的位置，因此它们之间的 F1 接口通过应用网络域安全/互联网协议（NDS/IP）来保护。同样地，在 NDS/IP 基础上，gNB-CU-CP 和 gNB-CU-UP 之间的 E1 接口安全得到保障。将 gNB 连接到核心网络的回程网络通过使用 NDS/IP 得到保护，除非回程网络中有物理保护。由于用户平面功能（UPF）可以部署在网络边缘，因此 UPF 和会话管理功能（SMF）之间的通信也通过使用 NDS/IP 来保护。以下简要概述与接入网的安全架构相关的安全服务或功能：

– 用户隐私；
– 认证；
– 密钥层次结构；
– NAS信令、AS信令和用户数据的安全性；
– NDS/IP；
– 非3GPP接入安全性。

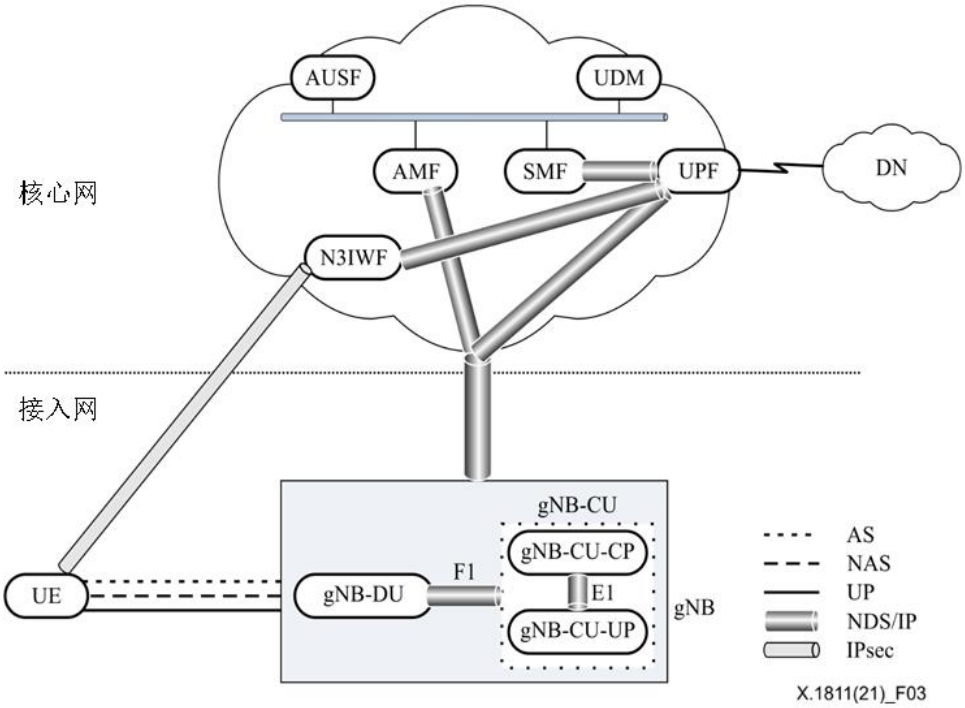


图3 – 接入网的安全架构

7.2.1.1 用户隐私

在 IMT-2020 系统中，为 UE 分配一个全球唯一订购永久标识符（SUPI），该标识符将在通用用户身份模块 USIM 和统一数据管理/用户数据存储库（UDM/UDR）中提供。当部署 IMT-2020 USIM 时，SUPI 永远不会在空中接口上透明传输。对于初始接入，UE 生成订购隐藏标识符（SUCI），并将其传送至 UDM/ARPF（统一数据管理/认证证书存储库和处理功能），如图 4 所示。在接收到 SUCI 之后，位于 ARPF/UDM 的订购标识符去隐藏功能（SIDF）对来自 SUCI 的 SUPI 进行去隐藏。基于 SUPI，UDM/ARPF 根据订购数据选择认证方法。

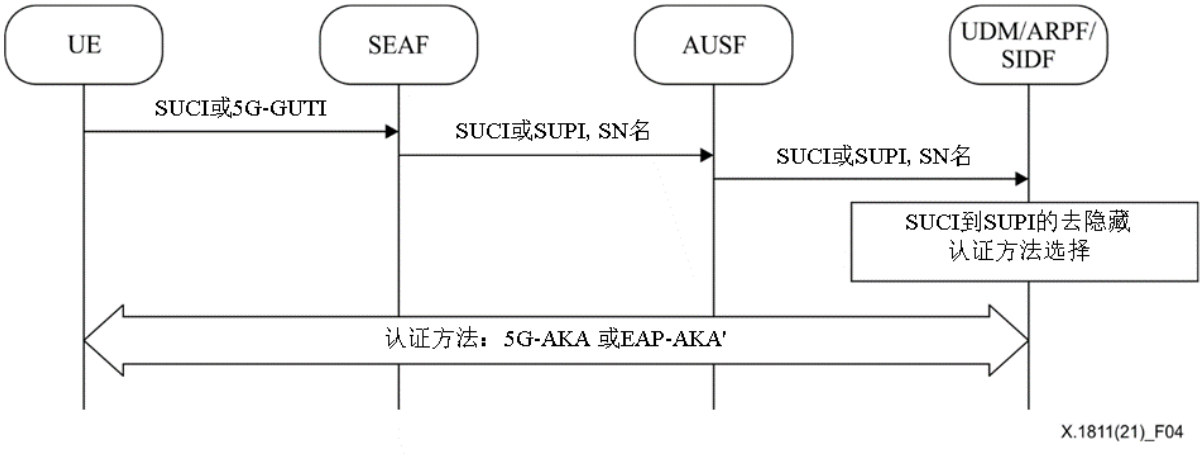


图4 – 初始认证程序和认证方法选择（改编自[b-3GPP TS 33.501]图6.1.2-1）

SUCI 由透明部分和加密部分组成。前者包含移动国家代码和移动网络代码，作为关于将 SUCI 路由到目标 UDM/ARPF 的归属网络的信息。后者包含敏感订购信息，即移动标识号（使用椭圆曲线集成加密方案（ECIES）进行加密）。归属网络的公共密钥分别在 USIM 和 SIDF 安全地提供。ECIES 的原理是，UE 和网络应用它们自己的私钥和伙伴公钥，通过使用 ECDH 机制就共享密钥达成一致。基于共享密钥，分别使用对称加密算法和 MAC 算法来执行数据保密性和完整性保护。根据[b-3GPP TS 33.501]中规定的配置文件（profiles），ECDH 机制（X25519，椭圆曲线辅因子 DH 原语）用于生成共享密钥，计数器模式下的 AES-128 和 HMAC-SHA-256 分别用于数据保密性和数据完整性。

在认证程序开始之后，以安全方式为 UE 分配一个 IMT-2020 全球唯一临时标识符（IMT-2020-GUTI），以在随后的认证过程中隐藏 SUPI。

7.2.1.2 认证

IMT-2020 系统采用 5G-AKA 和可扩展认证协议-认证和密钥商定（EAP-AKA'）两种 AKA 协议进行 UE 和网络之间的相互认证以及会话密钥 K_{SEAF} 的生成。后一协议可用于 3GPP 和非 3GPP 接入。与 4G 相比，IMT-2020 认证协议提供了更强的归属控制，以减轻漫游网络可能的欺诈性收费。在 EAP-AKA'的情况下，在归属网络的认证服务器功能（AUSF）处执行网络侧的 UE 身份验证。在 5G-AKA 的情况下，虽然网络侧 UE 身份验证是在漫游网络的安全地锚功能（SEAF）处执行的，但是归属网络的 AUSF 将在每个认证过程中验证认证确认。

在认证过程中使用一组密钥生成算法（*f*1、*f*1*、*f*2、*f*3、*f*4、*f*5 和 *f*5*）来生成认证矢量（AV）和认证响应。对此有两种算法集可用。其中一个被称为米莱内奇（MILENAGE）算法集[b-ETSI 135 205]，其中 AES-128 被推荐为基础。另一个称为 TUAK 算法集[b-ETSI 135 231]，其中 Keccak 海绵函数（Keccak sponge function）[b- Bertoni]用作基础，其输入密钥规模可以是 128 位或 256 位。请注意，在实践中，MILENAGE 算法集比 TUAK 部署得更广泛。

7.2.1.3 密钥层次结构

基于根密钥 K，UE 和网络进行相互认证，并生成会话密钥 K_{SEAF}，该密钥是用于保护 UE 和网络之间通信密钥（K_{N3IWF}、K_{NASint}、K_{NASenc}、K_{RRCint}、K_{RRCenc}、K_{UPint}、K_{UPenc}）安全的地锚，具体见图 5。

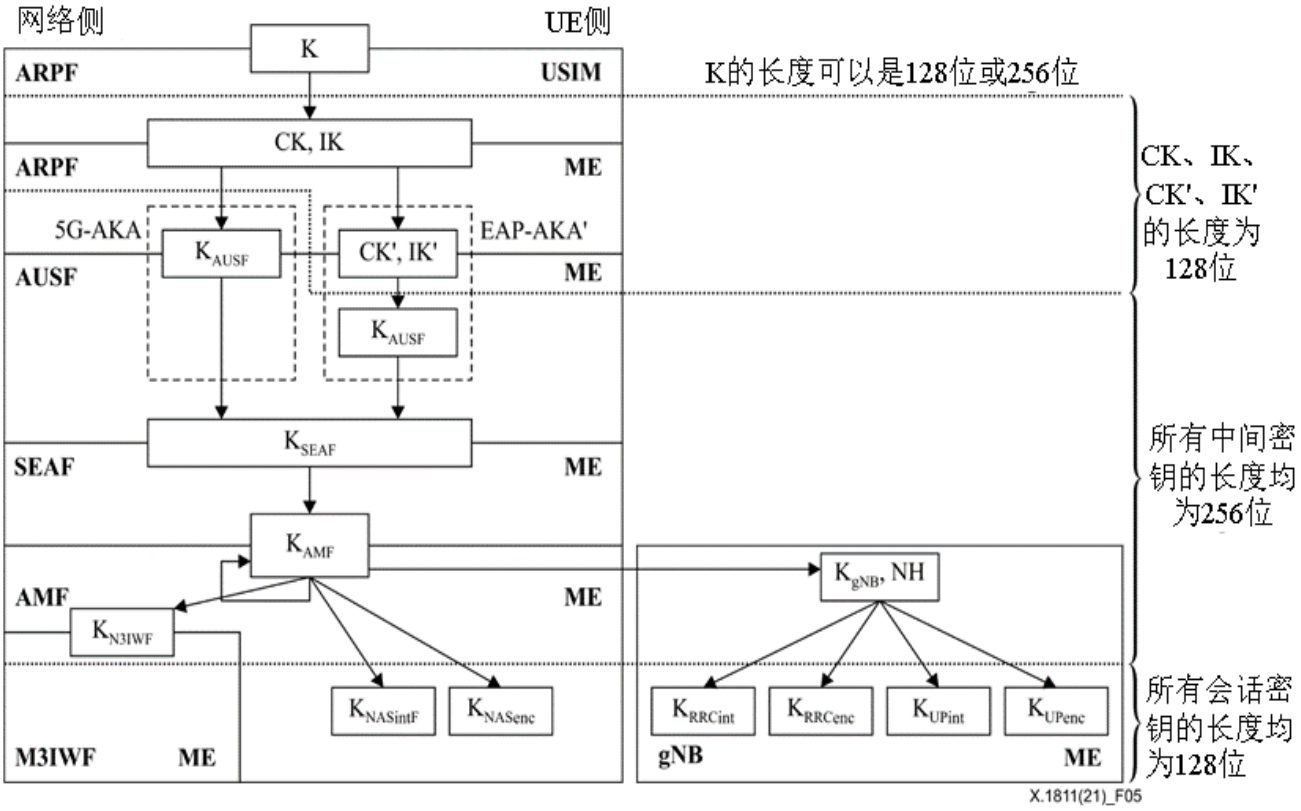


图5 – 密钥层次结构（改编自[b-3GPP TS 33.501]图6.2.1-1）

根密钥 K 的长度可以是 128 位或 256 位。值得注意的是，传统 USIM 中的根密钥 K 只有 128 位长，这意味着在 UDM 中只为相应的 USIM 提供了 128 位长的根密钥。

CK、IK、CK'和 IK'是与认证程序相关的密钥，长度为 128 位。CK 和 IK 的生成依赖于 MILENAGE 或 TUAK 算法集，而[b-3GPP TS 33.220]中定义的通用密钥推导函数（GKDF）用于生成 CK'和 IK'。

所有中间密钥的长度都是 256 位，其生成依赖于 GKDF，EAP-AKA'协议中的密钥 K_{AUSF} 除外。[b-IETF RFC 5869]中规定的基于 HMAC 的提取和扩展密钥推导函数（HKDF）用于生成 EAP-AKA'协议中的 K_{AUSF}。

用于保护 UE 和网络之间通信安全的密钥（K_{N3IWF}、K_{NASint}、K_{NASenc}、K_{RRCint}、K_{RRCenc}、K_{UPint}、K_{UPenc}）长度为 128 位，从 GKDF 的 256 位输出中截断取用。

7.2.1.4 NAS信令、AS信令和用户数据安全性

为了确保 NAS 信令、AS 信令和用户数据的保密性，IMT-2020 系统须支持 128-NEA1（基于 128 位 SNOW 3G 的算法）和 128-NEA2（基于 128 位 AES 的算法）。此外，IMT-2020 系统中可支持 128-NEA3（基于 128 位 ZUC 的算法）。

为了确保 NAS 信令、AS 信令和用户数据的完整性，IMT-2020 系统须支持 128-NEA1（基于 128 位 SNOW 3G 的算法）和 128-NEA2（基于 128 位 AES 的算法）。此外，IMT-2020 系统中可支持 128-NEA3（基于 128 位 ZUC 的算法）。

7.2.1.5 NDS/IP

接入网和核心网之间的接口（即 gNB 和 AMF 之间的 N2 接口、N3IWF 和 AMF 之间的 N2 接口、gNB 和 UPF 之间的 N3 接口、N3IWF 和 UPF 之间的 N3 接口)、gNB-DU 和 gNB-CU 之间的接口（F1 接口）、gNB-CU-CP 和 gNB-CU-UP 之间的接口（E1 接口）通过应用 NDS/IP（[b-3GPP TS 33.210]、[b-3GPP TS 33.310]）进行保护，这一协议规定了 3GPP 系统中用于 IPsec、互联网密钥交换版本 2（IKEv2）、TLS 和数据报传输层安全（DTLS）的安全配置文件[b-IETF RFC 6083]。

为了保护通过 N2 接口、E1 接口和 F1 接口传输的数据的完整性和保密性，并防止重放攻击，建议实施 IPsec 封装安全有效载荷（ESP）和基于 IKEv2 证书的认证。此外，须支持 DTLS。

为了对 N3 接口上的流量提供完整性、保密性和重放保护，建议实施 IPsec ESP 和基于 IKEv2 证书的认证。

作为 ESP 加密算法，除了 AES-256 之外，还须支持高级加密标准-密码块链接（AES-CBC）和高级加密标准-伽罗瓦计数器模式（AES-GCM），该模式具有 16 个八位字节的 ICV。作为 ESP 认证算法，须支持 HMAC-SHA1-96 和具有 AES-128 的高级加密标准-伽罗瓦消息认证码（AES-GMAC）。

关于 IKEv2，须支持以下算法：

– 保密性：密钥长度为128位的ENCR_AES_CBC、具有16个八位字节ICV且密钥长度为128位的AES-GCM；

– 伪随机功能：PRF_HMAC_SHA1、PRF_HMAC_SHA2_256；

– 完整性：AUTH_HMAC_SHA256_128；

– DH组14（2 048位MODP）、19（256位随机ECP组）；

关于 IKEv2，为了实现高安全级别，应支持以下算法：

– 保密性：具有16个八位字节ICV且密钥长度为256位的AES-GCM；

– 伪随机函数：PRF_HMAC_SHA2_384；

– DH组20（384位随机ECP组）。

DTLS 1.2 与 TLS 1.2 共享相同的密码套件，因为如[b-IETF RFC 6347]所述，DTLS 1.2 是基于 TLS 1.2 的。须遵循 TLS 1.2 [b-IETF RFC 5246]中给出的允许和强制密码套件。此外，以下密码套件是强制支持和建议使用的：

– [b-IETF RFC 5289]定义的TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256；

– [b-IETF RFC 5288]定义的TLS_DHE_RSA_WITH_AES_128_GCM_SHA256。

为了实现高水平的安全性，建议支持以下密码套件：

– [b-IETF RFC 5289]定义的TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384；

– [b-IETF RFC 5289]定义的TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384。

关于 DH 组，对于 ECDHE，须支持[b-IETF RFC 4492]中定义的曲线 secp256r1（P-256）；应支持[b-IETF RFC 4492]中定义的 secp384r1（P-384）。对于 DHE，应支持至少 4 096 位的 DH 组；不得支持小于 2 048 位的 DH 组。

允许在 NDS/IP 环境下的 IKEv2、TLS 握手中使用基于 PSK 的认证。

7.2.1.6 非3GPP接入安全性

非 3GPP 接入的安全性是通过在 UE 和 N3IWF 之间建立 IPsec 隧道来实现的。IKEv2 [b-IETF RFC 7296]用于在密钥 K_{N3IWF} 的基础上执行 UE 和 N3IWF 之间的相互认证，以便为 IPsec 隧道建立一个或多个 IPsec ESP [b-IETF RFC 4303]安全关联。

N3IWF 与 AMF（N2 接口）以及 N3IWF 与 UPF（N3 接口）之间的通信安全通过使用 NDS/IP 得到保障。

7.2.2 核心网安全性

预计 IMT-2020 核心网络将在 NFV 框架[b-ETSI GS NFV 002]的基础上构建，其中网络功能（NF）与专用硬件分离，以实现快速服务部署并提高运营效率。如图 6 所示，NFV 框架可分为三层：NFVI、VNF 和网络服务。VNF 运行在通用 NFVI 层之上，以提供所需的网络服务。核心网络的安全性本质上是 VNF 层的安全性。

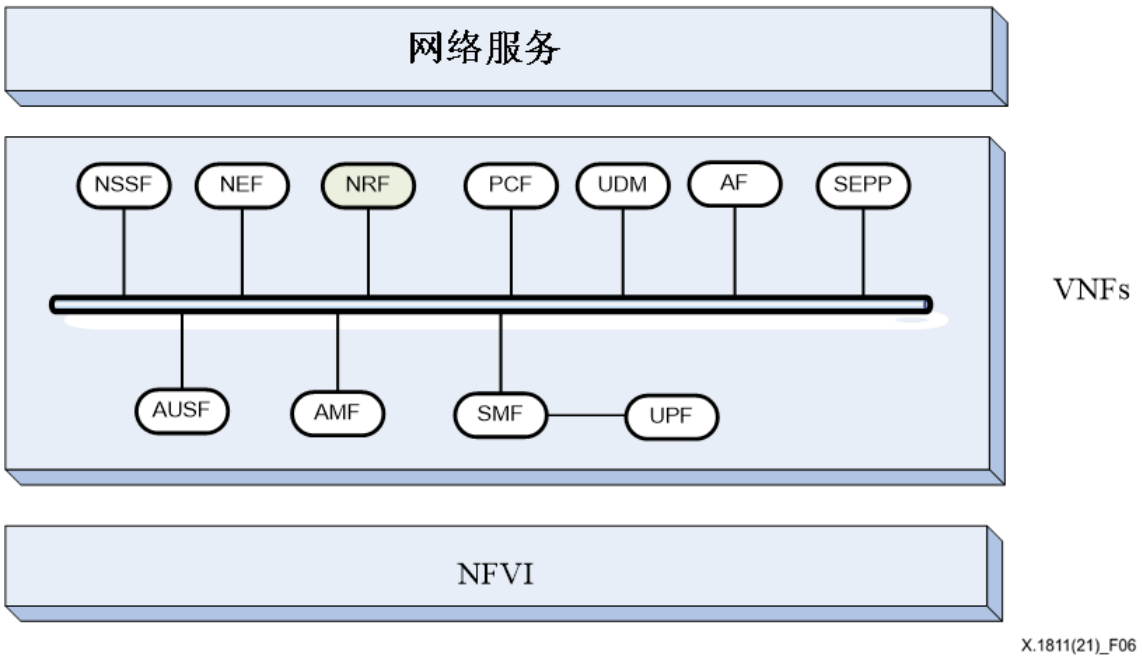


图6 – 基于NFV的IMT-2020核心网络框架
（改编自[b-ETSI GS NFV 002]图1）

VNF 在 SBA 中得到组织，其中 NF 存储库功能（NRF）在系统中发挥着关键作用。NRF 决定 NF 是否被授权执行发现和注册，并向 NF 发布接入令牌。VNF 层的安全性可分别在公众陆地移动网络（PLMN）内和 PLMN 之间进行考虑。

7.2.2.1 PLMN内

1) 认证

在发现、注册和接入令牌请求过程中，NRF 和 NF 须相互认证。这可以通过使用 NDS/IP 或物理安全来实现。NF 之间的认证可以以相同方式进行。

2) 授权

– 静态授权

在服务消费者 NF 和服务生产者 NF 相互认证之后，服务生产者 NF 在授予对服务应用编程接口（API）的访问之前，须基于本地政策查验服务消费者 NF 的授权。

– 基于OAuth 2.0的授权

NF 提供的网络服务访问控制可通过使用 OAuth 2.0 框架实现（[b-IETF RFC 6749]予以规定）。访问令牌须为[b-IETF RFC 7519]规定的 JavaScript 对象表示法（JSON）网络令牌 – 使用数字签名或基于[b-IETF RFC 7515]中所述 JSON 网络签名（JWS）的 MAC 数字签名得到保护。NRF 充当 OAuth 2.0 授权服务器。NF 服务消费者和 NF 服务生产者分别对应于 OAuth 2.0 客户机和 OAuth 2.0 资源服务器。NF 和 NRF 之间的通信通过使用 TLS 来保护，因为证书是在它们之间传送的。

7.2.2.2 PLMN间

如图 7 所示，通过 N32 接口，两个网络的安全边缘保护代理（SEPP）实现 PLMN 间的安全性。

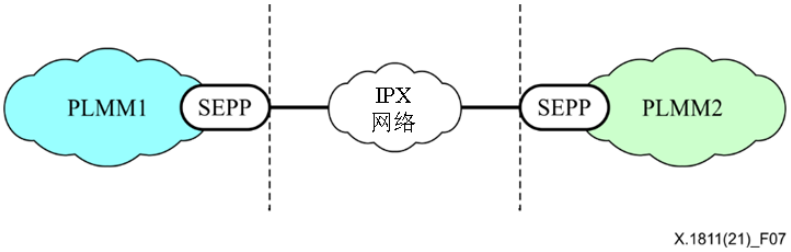


图7 – PLMN间安全性

N32 接口由 N32-c 连接和 N32-f 连接组成。前者负责 N32 接口的管理，包括通过使用 TLS 在两个 SEPP 之间建立相互 AKA。后者保证在 SEPP 之间发送受 Javascript 对象签名和加密（JOSE）保护的消息。

SEPP 使用 JSON 网络加密（JWE，[b-IETF RFC 7516]规定）保护 N32 接口上的消息，其中应用 N32-c 连接中的两个 SEPP 之间的商定密钥。IP 交换（IPX）提供商应用[b-IETF RFC 7515]中规定的 JWS 签署其中介服务所需的修改。

支持 JWE 的所有实体和功能都须使用以下算法[b-3GPP-TS 33.210]：“enc”参数 A128GCM（带 128 位密钥的 AES-GCM）且须得到支持。应支持“enc”参数 A256GCM（使用 256 位密钥的 AES-GCM）。须支持“alg”参数“dir”（直接使用共享对称密钥作为内容加密密钥（CEK））。

支持 JWS 的所有实体和功能均须使用以下算法[b-3GPP-TS 33.210]：“alg”参数 ES256（使用 P-256 的椭圆曲线数字签名算法（ECDSA）和安全散列算法-256（SHA-256））须得到支持。

7.3 管理平面安全性

管理平面由一组管理器（NFV 编排器、VNF 管理器、虚拟化基础设施管理器、SDN 控制器、RAN 管理器）组成。该组管理器通过接口负责相应目标的配置、性能和故障管理。在管理器和被管理目标之间的数据传输过程中，须防止任何修改、删除、插入或重放[b-ETSI GS NFV-SEC 014]。为此，行业默认将 TLS 应用于这些接口，具体见图 8。

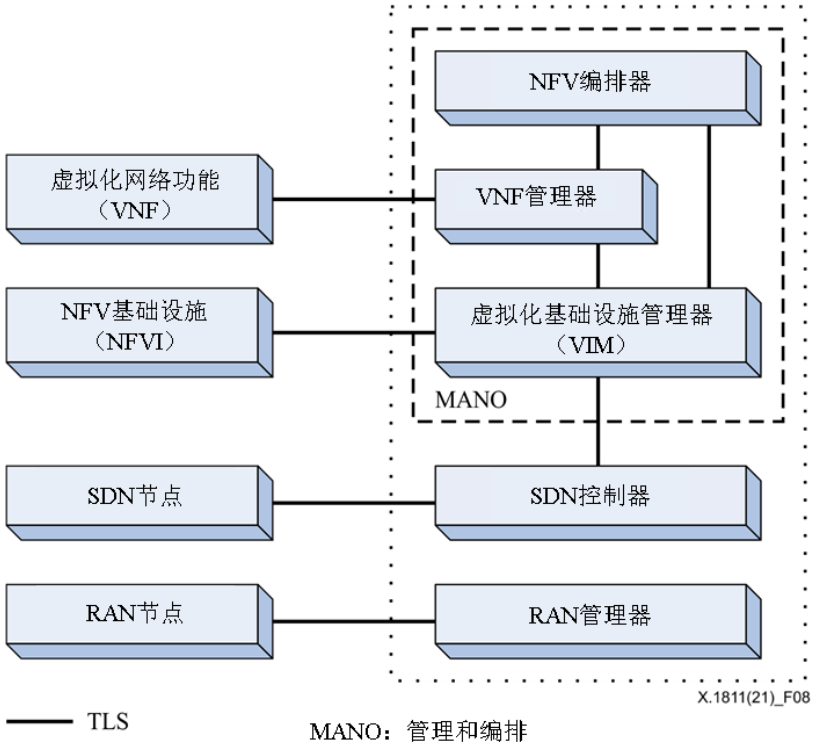


图8 – 管理平面安全性

7.4 IMT-2020系统所用密码算法总结

基于第 7.1 到 7.3 节对 IMT-2020 系统安全架构的介绍，表 1 总结 IMT-2020 系统中使用的密码算法。

表1 – IMT-2020系统中使用的密码算法

类型	名称	功能	应用情形
对称密码算法	128-NEA1	加密	UE和AMF之间以及UE和gNBUE之间的保密性保护
	128-NEA2		
	128-NEA3		

表1 – IMT-2020系统中使用的密码算法

	128-NIA1	MAC	UE和AMF之间以及UE和gNBUE之间的完整性保护
	128-NIA2		
	128-NIA3		
	AES-128	加密	IPsec、TLS、DTLS、JWE、ECIES、NFVI
	AES-256	加密	IPsec、TLS、DTLS、JWE、NFVI
	Blowfish	加密	SDN
	3DES	加密	SDN
	SHA-256	散列法	IPsec、TLS、DTLS、JWS、NFVI
	SHA-384	散列法	IPsec、TLS、DTLS、JWS、NFVI
	HMAC-SHA-256	密钥推导/MAC/伪随机函数	密钥层次结构IPsec、TLS、DTLS、JWS、NFVI
	HMAC-SHA-384	密钥推导/MAC/伪随机函数	IPsec、TLS、DTLS、JWS、NFVI
非对称密码算法	RSA	签名	IPsec、TLS、DTLS、JWS、NFVI
	ECDSA	签名	IPsec、TLS、DTLS、JWS、NFVI
	DH	密钥协议	IPsec、TLS、DTLS、NFVI
	ECDH	密钥协议	IPsec、TLS、DTLS、NFVI
注1 – 由于SHA-1的安全强度较弱，所以没有列出。 注2 – 当前使用的非对称密码算法密钥规模没有标记，因为如果可用大规模量子计算机，则无论密钥大小如何，这些算法都可能受到破坏。 注3 – 出于安全原因，TLS的版本不低于1.2。			

8 量子计算环境中IMT-2020系统的安全性评估

量子计算机是一种利用量子力学现象（叠加和纠缠）进行计算和操纵数据的设备。当前流行的密码算法的安全基础是建立在一些棘手的数学问题上的。由于量子计算机固有的并行属性，所以一些量子算法可以比经典算法更有效地解决困难的数学问题。这对当代密码学构成了严重而现实的安全威胁。附录 III 列出量子计算对常见密码算法的影响。在第 8.1 节中，介绍由于量子计算机的出现对传统密码算法造成的威胁。之后，分析量子计算机对 IMT-2020 系统的影响。

8.1 对传统密码算法的威胁

8.1.1 非对称密码算法

Shor 算法可在多项式时间内解决保理大整数分解问题和离散对数问题[b-Shor 1999]。这破坏了当前流行的非对称算法的安全性。这意味着基于 RSA 的公钥密码术（其安全性依赖于保理大整数分解问题）和 DH 密钥交换协议（其安全性依赖于离散对数问题）将不会提供安全性。像 DH 算法一样，DSA 算法的安全性依赖于离散对数。因此，DSA 算法容易受到量子攻击。ECC 的安全性依赖于椭圆曲线离散对数问题（ECDLP），与基于 RSA 的公钥系统相比，其密钥尺寸明显更小，因此已得到广泛部署。然而，使用 Shor 算法的一种变体即可将

之破解[b-Roetteler]。这意味着，如果有大规模量子计算机可用，则包括 ECDSA 和 ECDH 在内的 ECC 将是不安全的。表 2 列出破解目前广泛使用的非对称密码算法所需的量子资源。

表2 – 破解非对称密码算法所需的量子资源

算法	公共密钥规模（位数）	与对称算法相当的安全级别（位数）	逻辑量子位（qubits）	物理量子位（见注1）	托弗利门（见注1）	破解算法所需时间（见注2）
RSA [b-Häner]	1 024	80	2 050	7.38×10^6	5.81×10^{11}	9.68小时
	2 048	112	4 098	1.48×10^7	5.2×10^{12}	3天14小时
	4 096	128	8 194	2.95×10^7	5.59×10^{13}	31天21小时
基于ECC [Roetteler]	256	128	2 330	8.39×10^6	1.26×10^{11}	2.1小时
	384	192	3 484	1.25×10^7	4.52×10^{11}	7.5小时
	521	256	4 719	1.69×10^7	1.14×10^{12}	19小时
注1 – 量子计算机需要额外的物理量子位来进行纠错。每个逻辑量子位的物理量子位估计数量从10到10 000不等。这里我们假设每3 600个物理量子位有一个逻辑量子位，见[b-Fowler]。 注2 – 我们假设托弗利门的运行时间为60纳秒，见[b-Banchi]。						

8.1.2 对称密码算法

与经典算法相比，Grover 算法在非结构化数据集中提供了二次加速搜索[b-Grover]。这可以用来在对称密钥算法的密钥空间中搜索密钥。对于密钥长度为 n 位的对称密钥算法，可以用量子机器上的 $O(2^{n/2})$量子运算而不是常规计算机上的 $O(2^n)$经典运算找到密钥。搜索对称算法的密钥所需的量子资源巨大，所以在实际物理量子计算机上实施 Grover 算法以破解对称密钥算法是有问题的。例如，通过使用 Grover 算法为 AES 进行穷尽式的密钥搜索需要以下数量的 Toffoli 和 Clifford 门：AES-128 为 2^{86}；AES-192 为 2^{118}；AES-256 为 2^{151}，尽管所需的逻辑量子位数量在 3 000 到 7 000 之间[b-Grassl]。

Grover 算法将有效密钥大小减半，即它将对称密钥算法的安全强度减半。因此，为了实现量子辅助，对称密钥算法的密钥规模必须加倍。

8.1.3 散列算法

与经典算法相比，Grover 算法及其变体并没有加快散列冲撞的查找速度[b-Bernstein 2009]。最好的方式是在经典计算机群上使用 Pollard's ρ 方法的并行版本[b-ETSI GR QSC 006]。这意味着，如果目前使用的散列算法是安全的，那么在量子时代，它们也将是安全的，不会受到量子计算攻击。已证明使用经典计算是安全的 SHA-256 也被证明能够抵抗量子预镜像（pre-image）攻击[b-Amy]。

8.1.4 密钥推导函数

密钥推导函数（KDF）旨在生成用于保密性和完整性保护的密钥，这是通过将共享密钥嵌入散列函数来实现的。IMT-2020 系统中部署了两种 KDF。一种是[b-3GPP TS 33.220]中定义的 GKDF，另一种是[b-IETF RFC 5869]中规定的 HKDF。

GKDF 和 HKDF 的基础是键控散列函数 HMAC-SHA-256。HMAC 的安全性取决于所用散列函数的密码强度[b-IETF RFC 2104]。因此，IMT-2020 系统中使用的 KDF 本身并没有受到量子计算进步的实质性影响。

请注意，KDF 输出的熵取决于 KDF 中使用的输入密钥的熵。对于 256 位的熵输出，应用 KDF 时需要 256 位的熵输入密钥。

8.2 大规模量子计算机时间表的预测

很难预测提供大规模量子计算机的确切时间表，因为在这个问题上尚未达成共识。[b-NISTIR 8105]估计一台耗资 10 亿美元的量子计算机，可能在 2030 年破解 2 048 位 RSA。欧洲电信标准协会（ETSI）也得出了类似的结论，即大规模计算机可能在 2031 年建成[b-ETSI GR QSC 004]。因此，IMT-2020 系统的安全性可能会受到影响，因为 IMT-2020 系统将运行 10 到 20 年。另一方面，[b-NASEM]表明，在未来十年内，不太可能制造出破解 2 048 位 RSA 的量子计算机。这并不意味着现在不应该研究和对量子安全密码算法进行标准化，因为过渡到新的安全算法的时间框架足够长且不确定[b-NASEM]。

8.3 对IMT-2020系统的影响

如第 7 节所示，IPsec、TLS 和 DTLS 已部署在 IMT-2020 网络的许多地方。首先有必要给出一种总体观点来评估量子计算机对这些系统造成的威胁。之后，将根据第 7 节中介绍的结构评估对 IMT-2020 系统安全性的影响。

8.3.1 对IPsec、TLS和DTLS的影响

尽管 IPsec、TLS 和 DTLS 在不同层上运行以保护消息传输（IPsec 位于网络层，TLS 和 DTLS 位于网络层和应用层之间），但它们的设计遵循相似的原则。它们由两部分组成：一部分是生成会话密钥的认证和密钥建立；另一部分是通过使用具有会话密钥的对称算法来保护消息的保密性和完整性。

现有两种执行认证和密钥建立的方法，其基础是：(1) 预共享对称密钥；(2) 公钥（通常使用证书）。

为进行保密性和完整性保护，目前 IPsec、TLS 和 DTLS 中的密码套件可支持 128 位和 256 位对称算法。

因此，可以通过考虑案例 1 到 4 来评估 IPsec、TLS 和 DTLS 是否能够抵御量子计算攻击。

案例 1：基于公钥的认证和 128 位或 256 位对称算法

在该案例中，会话密钥可被攻击者恢复，因为互联网工程任务组（IETF）标准中目前规范的不对称算法可由于 Shor 算法而被量子计算机破解。因此，无论对称算法的密钥尺寸有多长，被传输消息的安全性都无法得到保证。

案例 2：基于 128 位 PSK 的认证和 128 位对称算法

在该案例中，由于 Grover 算法，如果大规模量子计算机可用，则有效的安全密钥规模为 64 位。因此，这三个协议不能抵御量子攻击。

案例 3：基于 256 位 PSK 的认证和 128 位对称算法

在该案例中，虽然 256 位 PSK 用于认证和密钥建立，但只有 128 位对称算法应用于消息保护。因此，这三个协议的安全强度是 64 位。

案例 4：基于 256 位 PSK 的认证和 256 位对称算法

在该案例中，这三种协议的有效安全强度为 128 位。因此，可通过使用这种密码配置文件来挫败量子攻击。

对于当前的密码配置文件，只有案例 4 是安全的，不会受到量子攻击。但是，基于 PSK 的认证仅适用于小型通信群，因为 PSK 必须在相应的设备中手动配置。当通信群变大时，建议应用基于公钥的认证。为此，建议在上述协议（即 IPsec、TLS 和 DTLS）中引入量子安全密码非对称算法进行认证。

8.3.2 对基础设施层的影响

如第 7.1 节所示，TLS 用于保护应用和 SDN 控制器之间的接口，以及 SDN 控制器和 SDN 节点之间的接口。IPsec 可应用于 SDN 控制器和 SDN 节点之间的接口。根据第 8.3.1 段中的分析，这两个接口会受到量子攻击，即攻击者可以窃听、更改和注入通过这两个接口传输的消息，除非在 TLS 和 IPsec 中部署案例 4 所述算法。

NFVI 层容易受到量子攻击，因为它依赖经典非对称密码算法来实现一些安全功能。这可能会导致产生严重后果，如非法访问平台或植入恶意软件等。

8.3.3 对接入网的影响

8.3.3.1 用户隐私

如第 7.2 节介绍，采用 ECIES 方案，通过将 SUPI 转换为 SUCI 来对之进行隐藏。ECDH 用于在 ECIES 方案中商定 UE 和网络之间的共享密钥。如果大规模量子计算机可用，则攻击者可以恢复共享密钥。因此，通过用共享密钥解密 SUCI，会将 SUPI 泄露给攻击者。

8.3.3.2 认证

5G-AKA 和 EAP-AKA'协议都基于长期密钥 K 在 UE 和网络之间进行相互认证，长期密钥 K 的大小可以是 128 位或 256 位。至于 256 位密钥 K，到目前为止，还没有对散列函数（即 TUAK 算法集）的攻击，散列函数是通过使用经典计算机导出认证协议中使用的各种参数的基础。因此，这两种认证协议都是安全的，不会受到量子攻击，因为在 256 位 K 密钥环境中，使用量子计算机破解散列函数的算法比使用经典计算机更有效。至于 128 位密钥 K（其在量子时代的有效安全强度是 64 位），攻击者可以通过使用 Grover 算法执行 2^{64} 个量子运算来从与两种认证协议（例如 AV）相关的捕获消息中恢复密钥 K。

8.3.3.3 密钥层次结构

密钥层次结构用于从长时间（根）密钥 K 中导出 128 位密钥（如图 5 所示），以保护 UE 和网络之间的通信。目前广泛部署的是 128 位的密钥 K，很少应用 256 位的密钥 K。至于 128 位的 K – 在量子时代其有效安全强度是 64 位 – 导出的密钥的安全强度是 64 位。因此，攻击者可以从这些捕获的用 128 位密钥加密的消息中恢复密钥。

8.3.3.4 NAS信令、AS信令和用户数据

NAS 信令、AS 信令和用户数据的保密性通过使用具有 128 位长密钥的对称算法来保护。因此，攻击者可以用量子计算机解密这些消息。

NAS 信令、AS 信令和用户数据的完整性通过使用具有 128 位密钥的 MAC 算法来保护。MAC 算法的输出被截断为 32 位长的标签，用作 MAC 标签。很明显，如果 MAC 标签长度为 32 位，则攻击者可以在尝试 231 次后伪造消息。如果从 64 位本机标签或 128 位本机标签中截取一个 32 位长的 MAC 标签，是否会危及 IMT-2020 系统的安全性，则需要进行进一步研究。

8.3.3.5 NDS/IP

部署 TLS、DTLS 和 IPsec 是为了保护第 7.2.1 段中介绍的 N2 接口、N3 接口、E1 接口和 F1 接口。这造成了与传输层相同的影响，即如果不使用第 8.3.1 段案例 4 中的密码套件，则攻击者可以窃听、更改和插入通过这些接口传输的消息。

8.3.3.6 非3GPP接入安全性

非 3GPP 接入通过使用 IPsec 实现保护。出于第 8.3.1 段中介绍的原因，除非使用第 8.3.1 段案例 4 中的密码套件，否则无法保证安全的非 3GPP 接入。

8.3.4 对核心网的影响

8.3.4.1 PLMN内

1) 认证

如果 NF 的操作依赖于物理安全，则 NF 之间的认证不会受到影响。如果通过使用 NDS/IP 实现认证，则认证可能会受到第 8.3.3 段中所述的相同威胁的影响。

2) 授权

静态授权不会受到影响，因为不应用密码算法。

对于基于 OAuth 2.0 的授权，有两种可以确保访问令牌完整性的情形。如果通过使用签名来保护访问令牌的完整性，那么对手可以伪造访问令牌。相比之下，如果应用具有 256 位长密钥的 MAC 来保护其完整性，则访问令牌将不能被伪造。除非应用第 8.3.1 段中的案例 4，否则授权中使用的证书可在 NF 之间经 TLS 在传输时被披露。

8.3.4.2 PLMN间

攻击者可窃听、更改和注入通过 PLMN 之间的 N32 接口传输的消息，原因是 N32-c 连接依赖于 TLS 中基于证书的认证来建立会话密钥，所以攻击者可通过使用量子计算机来获取这些密钥。

8.3.5 对管理平面的影响

在管理器和被管理对象之间的数据传输过程中，任何修改、删除、插入或重放都是可能的，因为在管理平面中部署了具有基于证书认证的 TLS。这对 IMT-2020 系统构成了严重威胁，因为攻击者有可能访问到 IMT-2020 网络的管理系统。

9 量子安全密码算法

量子计算引入了一种全新的计算范式。尽管每种算法的影响程度不同，但都将影响对称密钥算法（如分组密码）和公钥算法（如 RSA）的安全性。

[b-Moses]表明，对于任何对称密钥算法，量子计算可有效地将密钥强度的位数减半且量子计算机可以运行算法（例如[b-Grover]算法），并在 $2^{N/2}$ 运算中用 N 位密钥找到对称加密的密钥。因此，如果量子计算成为现实，对称密钥算法可以通过简单地将密钥大小加倍来防止出现这种情况。当然，这将对对称密钥算法的性能产生影响。

至于 RSA、DSA、ECC、DH 等非对称密钥算法，我们认为量子计算的影响相当严重。量子计算机可以运行算法（例如[b-Shor 1997]算法），这些算法能在很短的时间内破解所有流行的公钥系统。例如，一种叫做肖尔（Shor）算法的量子算法可以在多项式时间内[b-Moses]恢复一个 RSA 密钥。

量子安全密码算法应根据评估标准进行选择（NIST 的评估标准见附录四）。

9.1 量子安全对称密钥算法

人们普遍认为分组密码或散列函数等基本对称密码系统属于量子安全算法[b-CSA]，见附录三。[b-ITU-T X.1197]提供了量子安全算法和密钥长度的示例表。与密码相关的量子计算机的出现尤其需要增加对称密钥的大小，相当于目前 IMT-2020 中使用的 128 位密钥的两倍。[b-CSA]显示，人们认为当前推荐的 256 位密钥大小是安全的，即使与 Grover 算法相比亦是如此。

9.2 量子安全的非对称密钥算法

如附录三所示，虽然量子计算机可以运行算法，在很短的时间内破解当前的公钥系统（如 RSA 和 ECC），但除了 RSA 和 ECC 之外（如第 9.2.1 至 9.2.5 段所述）还有许多重要的密码系统类别可以抵御量子计算机的攻击。[b-ITU-T X.1197]提供了量子安全非对称算法的现行标准列表。

注 – 量子密钥分发（QKD）是一种实现密钥协商的方法，已证明对量子计算具有鲁棒性。

9.2.1 基于格的算法

基于格的算法是基于有关格的一些众所周知的难题构造量子安全密码原语。最短向量问题（SVP）便是其中之一，即寻找给定格中的最短非零向量，此问题这已被证明是随机缩减下的非确定性多项式时间困难（NP-hard）问题[b-Ajtai]。

[b-CSA]表明基于格的算法可以提供数字签名、公钥或私钥加密和密钥协商。第 II.1 款列出了一些基于格的算法。

9.2.2 基于散列的算法

基于散列的算法依赖于底层加密散列函数的安全性。

[b-CSA]表明基于散列的算法用于使用散列函数构造的数字签名。第 II.2 款条列出了一些基于散列的算法。

9.2.3 基于代码的算法

基于代码的算法依赖于一些纠错码，即使对量子计算机而言，编码方案亦很难有效解码。比如 McEliece 密码系统[b-McEliece]就是基于一般线性码解码的 NP 难题。

[b-CSA]表明基于代码的算法可以提供数字签名、公钥或私钥加密和密钥协商。第 II.3 款列出了一些基于代码的算法。

9.2.4 多元算法

多元算法是基于在有限域内求解非线性多元多项式方程组这一难题。此问题已知具备 NP 难题属性[b-Garey]。

[b-CSA]表明多元算法可以提供数字签名和公钥或私钥加密。第 II.4 款列出了一些基于多元算法的实用签名方案。

9.2.5 基于超奇异同源的算法

超奇异同源的算法的构造是基于恢复一对已知为同源的，超奇异椭圆曲线间未知同源的困难性。

此算法提供了完美的前向安全性，并作为 DH 和 ECDH 方法的简单抗量子计算的替代品。一个典型的示例为超奇异同源 Diffie-Hellman（SIDH）算法[b-Jao]。

10 IMT-2020系统量子安全密码算法的使用导则

将量子安全非对称算法引入 IMT-2020 系统时，一般首先要考虑如何处理显著增加的消息量。随后将考虑量子安全加密算法在 IPsec、TLS 和 DTLS 中的使用，因为其已在 IMT-2020 系统的多处部署。接下来将分别阐述量子安全密码算法应用于 IMT-2020 接入网和 IMT-2020 核心网的导则。

10.1 消息的大小

包含公钥、密文或签名的消息的大小将显著增加，因为量子安全非对称算法通常比经典非对称算法更大，其内容与公钥、密文或签名相关。例如，量子安全非对称算法的公钥从 726 字节到大约 1 兆字节不等（见如第 II.5 款），而经典非对称算法的公钥大小通常从 32 字节到 256 字节不等。国家标准与技术研究所（NIST）计划实现一种以上量子安全不对称算法的标准化。因此，在 IMT-2020 系统中，需要很直观的选择具有较小公钥、密文或签名大小的量子安全非对称算法。此外，在部署量子安全非对称算法时，IMT-2020 系统标准需要为容纳公钥、密文或签名确定适当的消息大小。

10.2 IPsec、TLS和DTLS

如果将 PSK 应用于认证和密钥协议，则建议将 PSK 的大小定为 256 位并建议使用密钥长度为 256 位的量子安全对称算法，以保护通过网络传输的消息的机密性和完整性。如果使用基于证书的身份认证方案，建议将量子安全非对称算法集成至身份认证协议中，以实现量子安全身份认证和会话密钥协议。为保护消息的机密性和完整性，建议部署 256 位的长密钥量子安全对称算法。这样，SDN、NDS/IP 和管理平面都不容易受到量子攻击。

由于 NIST 尚未最终确定量子安全非对称算法的候选方案，IETF 还没有开始研究如何将量子安全算法添加到 IPsec、TLS 和 DTLS 的密码套件中。预计 NIST 标准草案将于 2022 年至 2024 年发布。一旦 IETF 为 IPsec、TLS 和 DTLS 指定了抗量子密码套件，考虑到稀缺的无线带宽和设备有限的计算能力，建议在 IMT-2020 系统中部署一个密钥更小、加密操作速度更快的密码套件。

10.3 基础设施层

建议使用 SDN 将第 10.2 款中规定的建议应用于 IPsec 和 TLS 的使用。

建议用量子安全加密算法替换部署在 NFVI 层的经典加密算法，包括对称和非对称类型的算法。

10.4 IMT-2020接入网

10.4.1 签约用户的隐私

建议 ECIES 方案应用类似 DH 的量子安全非对称算法生成共享密钥，如超奇异同代密钥封装（SIKE）和 NewHope，这些密钥是 NIST 后量子加密（PQC）标准化程序的第二轮候选方案（见附录二）。建议使用 256 位共享密钥的量子安全对称算法隐藏 SUCI。

10.4.2 认证

由于 MILENAGE 算法集仅支持 128 位密钥输入，而 TUAK 算法集可以支持 256 位密钥输入中的一种，因此建议在身份认证过程中使用 TUAK 算法集生成 AV 和身份认证响应，而不使用 MILENAGE 算法集。

10.4.3 密钥层级

为生成 256 位熵的会话密钥 K_{SEAF}，密钥层级必须进行以下调整：(1) 建议根密钥 K 的密钥大小为 256 位；(2) 建议不再截断 GKDF 的 256 位长输出。

实际上，根密钥 K 的密钥长度通常是 128 位，因为使用这种配置的 IMT-2020 系统使用了传统的 USIM 卡；许多运营商用于早期 IMT-2020 系统的新 USIM 卡仍将只存储 128 位根密钥。因此，从密钥 K 导出的会话密钥 K_{SEAF} 的熵只有 128 位，不具有量子安全性。

当 USIM 卡配备有 128 位长的根密钥时，为增强当前会话密钥 K_{SEAF} 的安全性，当前会话密钥 K_{SEAF} 的生成不仅基于由长期密钥 K 确定的第一会话密钥 K_{SEAF}'，还基于至少一个附加密钥。附加密钥可以是用户设备第一次连接到网络时生成的初始会话密钥 $K_{SEAF\_INITIAL}$ 和/或前一会话中使用的会话密钥 K_{SEAF_PRV}。第一会话密钥和附加密钥都是对称密钥，这意味着 UE 和网络共享这些密钥。这样，当前会话密钥 K_{SAEF} 的熵至少为 256 位，因为第一会话密钥 K_{SEAF}'的熵为 128 位，而附加密钥（密钥 $K_{SEAF\_INITIAL}$ 和/或密钥 K_{SEAF_PRV}）的熵至少为 128 位。

作为一种良好实践，新 SIM 卡可以选择性地用于实现会话密钥 K_{SEAF} 的 256 位熵。这些卡可以是 SIM 卡、USIM 卡或电子 SIM 卡，也可以使用其他非标准的 SIM 卡外形规格和类型，但应进行相应的调整，以便：

a) 存储一个256位的根密钥，使其起到与旧（U）SIM中的根密钥K相同的作用。

b) 支持新SIM卡中必要的KDF和对称加密核心（例如AES）环的硬件加速。这对于物联网和功能手机在蜂窝设备总数中占重要部分的国家关系已尤为密切，可以通过频率复用和协议转换与实现量子安全（如果并非快速）的IMT-2020兼容。

10.4.4 NAS信令、AS信令和用户数据的安全性

如第 7 款所示，AES-128、SNOW 3G 和 ZUC-128 等 128 位对称密钥算法，是 IMT-2020 接入网 NAS 信令、AS 信令和用户数据安全性的基础。

为抵抗量子攻击，建议在 IMT-2020 系统中部署 256 位的对称密钥算法。较长的 MAC 可以更好地抵御正确猜出消息 MAC 的量子攻击。[b-NIST SP 800-38B]建议使用至少 64 位的 MAC 来抵御猜测攻击。IMT-2020 接入网中的 MAC 长度只有 32 位。如果 MAC 大小从 32 位增加到 64 位，对 IMT-2020 网络和协议的影响很大。当应用 256 位量子安全对称算法生成 32 位长的 MAC 时，IMT-2020 接入网是否仍能抵御猜测攻击仍需进一步研究。

10.4.5 非3GPP接入的安全性

鉴于非 3GPP 接入的安全性依赖于 IPsec，因此非 3GPP 接入的抗量子攻击策略请参见第 10.2 款。

10.5 IMT-2020核心网

10.5.1 PLMN内部

1) 认证

为了抵抗量子攻击，建议基于 NDS/IP 的身份认证应用第 10.2 款中介绍的策略。

2) 授权

建议在 OAuth 2.0 中部署量子安全的键控散列函数（如 HMAC-SHA-256）以及量子安全签名算法，以确保访问令牌的完整性。关于传输到 TLS 中量子安全密码套件的策略，请参见第 10.2 款。

建议为 JWS 部署量子安全签名算法。

10.5.2 跨PLMN

建议将第 10.2 款中介绍的方法应用于 N32-c，以防止量子攻击者获得会话密钥。建议在 N32 接口中部署 256 位密钥的 AES-GCM，以确保 PLMN 之间通信的机密性和完整性。

建议为 JWS 部署量子安全签名算法而非 ECDSA。

附录一

IMT-2020系统概述

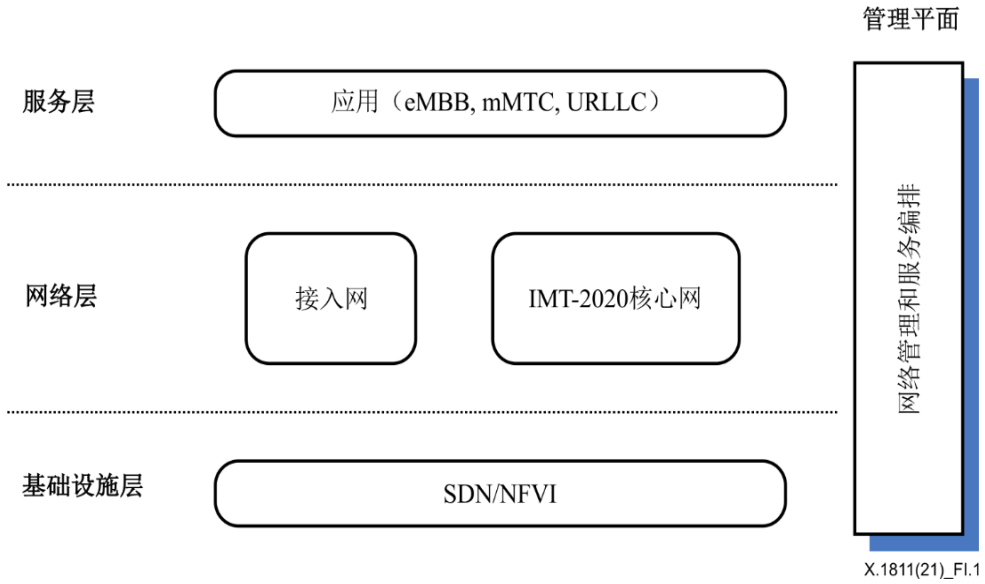
（本附录不构成本建议书的组成部分。）

本附录为IMT-2020系统概述。

I.1 总体架构

IMT-2020 系统旨在提供有不同性能要求的广泛服务。IMT-2020 网络提供的服务按照 3GPP 规范可以分为三类：(1) eMBB 支持比 4G/LTE 更高的数据速率和更高的用户移动性；(2) mIoT 提供大量的机器类通信；(3) URLC 支持可靠性要求更高和更低延迟的任务关键型服务。IMT-2020 系统将是一个灵活的平台，支持新的业务案例并集成了汽车、制造、能源、电子健康和娱乐等垂直行业。此外，与前几代移动网络相比，IMT-2020 系统的部署和维护更加容易。为了满足这些挑战性的要求，IMT-2020 系统引入了许多创新技术，如网络切片、NFV、SDN、SBA 和中央单元/分布式单元（CU/DU）分离。

如图 I.1 所示，IMT-2020 系统的总体架构可以分为：基础设施层；网络层；服务层和管理平面。



图I.1 – IMT-2020系统的总体架构

– 基础设施层包括SDN和NFVI。SDN用于将数据包传至目的地。除传统传输技术（例如，多协议标签交换（MPLS））外，IMT-2020系统还引入了SDN技术，以实现更高的传输速度同时更容易适应服务需求。NFVI是运行VNF的共同基础。

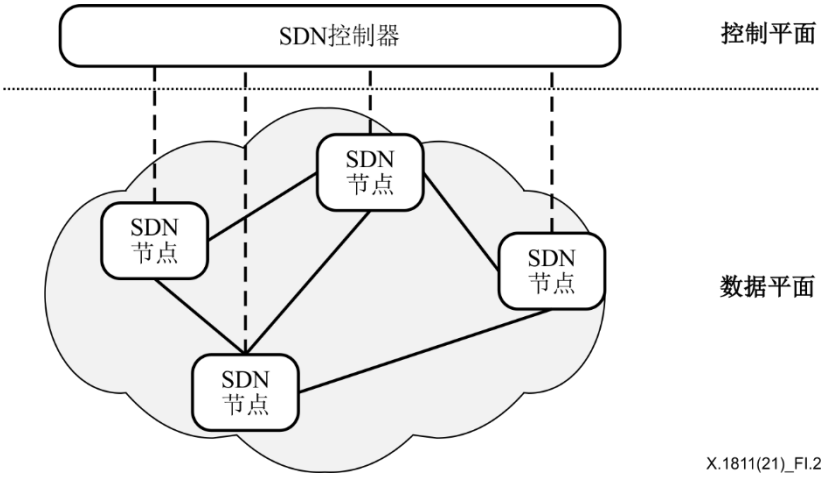
– 网络层由接入网和核心网组成。前者允许用户设备在任何地方接入IMT-2020网络。后者是在考虑到SBA的情况下为了扩展性和简单性而设计。核心网由许多支持数据连接和服务部署的NF组成，如AUSF、AMF和SMF。

– 服务层由在IMT-2020系统内运行的应用程序组成，可能是eMBB应用程序、大型机器类型通信（mMTC）应用程序和URLLC应用程序。

– 管理层负责网络管理和服务编排。

I.2 SDN

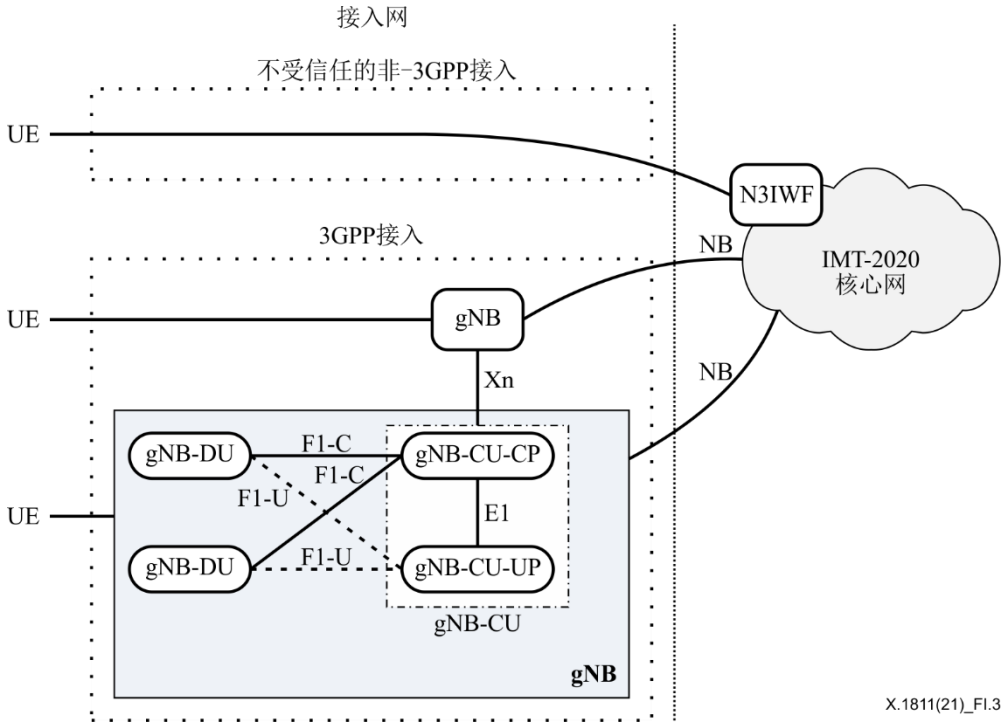
SDN 的基本原理是数据平面与控制平面（CP）解耦，使其能够支持网络节点在数据转发过程中的动态可编程性。SDN 控制器做出连网决策，并将生成的转发规则发送给网络节点。这种转发机制简化了网络节点的实现，并增强了数据平面的性能。SDN 架构如图 I.2 所示。



图I.2 – SDN架构

I.3 接入网

如图 I.3 所示，UE 可以采用不可信的非 3GPP 接入方式或 3GPP 接入方式接入 IMT-2020 核心网络。接入网络提供与无线接口数据传输相关的服务。



图I.3 – 接入网

– **不受信任的非3GPP接入**

不受信任的非3GPP接入是指并非GPP规定亦非IMT-2020核心网所信任的一种接入技术，如无线局域网（WLAN）接入。在这种情况下，用户设备通过N3IWF连接到IMT-2020核心网。

– **3GPP接入**

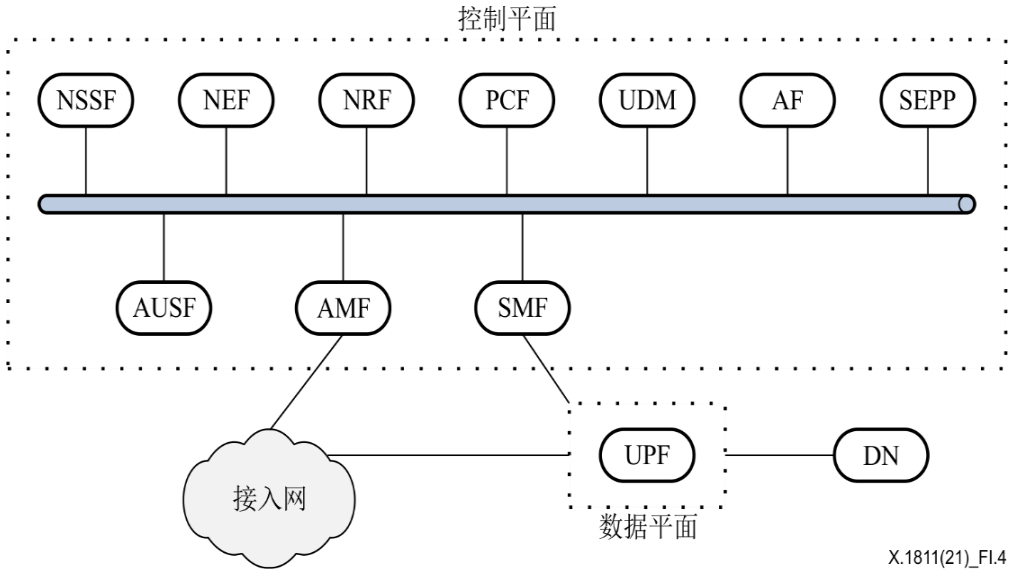
3GPP接入是3GPP规定的接入技术，即IMT-2020环境下的下一代无线接入网（NG-RAN）技术。用户设备可以通过使用NG接口通过一个扁平的gNB接入IMT-2020核心网络，而不需要分离CU/DU。NG接口是一种逻辑接口，支持在gNB和IMT-2020核心网之间交换CP信息和UP信息。为提高网络部署的灵活性并降低成本，gNB可以分为gNB-DU和gNB-CU。gNB-CU是一个逻辑节点，使用更高层协议，包括服务数据适配协议（SDAP）、无线电资源控制（RRC）和分组数据汇聚协议（PDCP）。gNB-DU是一个逻辑节点，负责执行更低层的功能，其中包括无线链路控制（RLC）、媒体访问控制（MAC）和物理层功能。

借用SDN概念，gNB-CU可进一步分为gNB-CU-CP和gNB-CU-UP。这将导致用户和CP实体之间的无线接入功能分解。CP和UP的这种分离提供了操作和管理复杂网络的灵活性，支持不同的网络拓扑、资源和新的服务需求。

gNB-CU和gNB-DU单元通过F1逻辑接口连接，可以区分用于连接gNB-CU-CP的F1-C接口和用于连接gNB-CU-UP的F1-U接口。gNB-CU-CP通过E1接口与gNB-CU-CP通信。

I.4 核心网

IMT-2020 核心网络定义为 SBA，见图 I.4。SBA 已经定义了许多 NF，服务于不同的目的。每个 NF 公开一组名为 NF 服务的服务，供其他授权的 NF 使用。NF 通过查询 NRF)相互寻找并通信。



图I.4 – IMT-2020核心网

IMT-2020 核心网可以分为 CP 和 UP。

– **控制平面**

此平面提供网络控制服务，包括接入、移动、政策、披露、合法监听和与收费相关的控制。控制平面定义了以下NF。

– **网络切片选择功能**（NSSF），用于选择为用户设备服务的网络切片实例集。

– **网络披露功能**（NEF），支持披露能力和事件。NF通过NEF向其他NF披露功能和事件。NF披露的功能和事件可以安全地向第三方、应用功能和边缘计算披露。

– **NF存储库功能**（NRF），提供注册和发现功能，以便NF可以通过API相互发现并相互通信。

– **政策控制功能**（PCF），支持通过统一的政策框架管理网络行为。

– **统一的数据管理**（UDM），存储用户数据和配置文件。UDM也用于为3GPP AKA生成AV。

– **应用功能**（AF），为提供服务与3GPP核心网络互动。AF还向PCF提供关于分组流的信息。

– **安全边缘保护代理**（SEPP），一种不透明的代理，用于保护在PLMN间CP接口上交换的消息，并隐藏PLMN内部网络的拓扑。

– **认证服务器功能**（AUSF），处理3GPP接入和非3GPP接入的认证请求。

– **接入和移动性管理功能**（AMF），为用户设备提供认证、授权和移动性管理。

– **会话管理功能**（SMF），用于会话管理，例如会话建立、修改和释放。SMF还向用户分配IP地址。

– 用户平面

用户平面功能（UPF）是为UP定义的唯一功能。UPF支持与UP数据包相关的各种操作和功能，如数据包路由和转发、流量处理、数据包检查和数据包复制。

IMT-2020核心网与上一代移动网络的核心网络有显著不同，具有以下特点。

– **SBA**，其服务操作比传统网络的运行粒度更细并且彼此松散耦合。这使得新服务的推出时间更短，系统更新的灵活性更大。

– **控制平面和用户平面分离**，允许UPF部署在更靠近用户设备的地方，从而满足URLLC服务的严格延迟要求。控制平面和用户平面的分离亦使得每个平面的资源能够独立缩放。

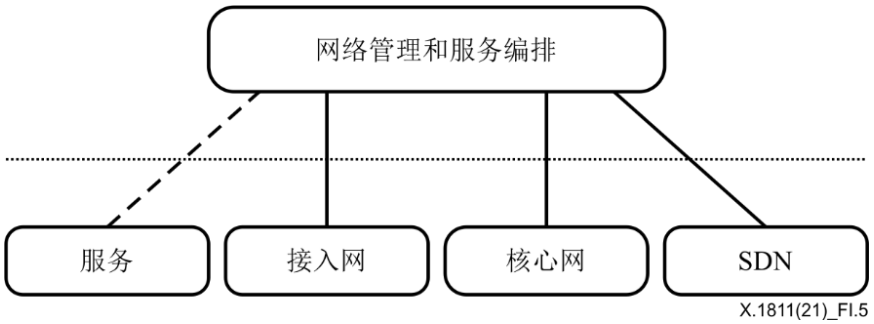
– **AMF和SMF分离**，允许以集中的方式实施访问和移动性管理。相比之下，SMF可位于服务有需要的地方。

– **NFV**，IMT-2020核心网在此假设以虚拟化方式实施NF，以更好的管理资源和成本节约。分离硬件和软件的NFV通过尽量减少对硬件约束的依赖，使网络更加灵活简单。

– **网络切片**，目的是让公共物理网络基础设施支持多种服务类型。网络切片可提供定制的端到端网络，以满足不同需求。根据服务要求，每个网络片可能包含不同的NF。

I.5 管理层

管理平面负责网络管理和服务编排。为了管理和监控网络，管理平面通过单独的专用通信通道连接到接入网、核心网和SDN，如图I.5所示。网络管理至少具有以下功能：故障管理（FM）、性能管理（PM）、配置管理（CM）和跟踪管理（TM）。除这些网络管理功能，网络切片的管理还需要以下功能：切片生命周期管理、切片能力管理和网络资源发现。服务编排应用灵活的资源控制和监控机制提供、管理和重新优化网络服务。



图I.5 – 一般管理架构

附录二

量子安全的非对称密钥加密算法

（本附录不构成本建议书的组成部分。）

本附录列出了众所周知的量子安全非对称密钥加密算法。

II.1 基于格的算法

一些基于格的算法如下：

– 第N次截断多项式环（NTRU）[b-Hoffstein]；
– 错误学习（LWE）[b-Regev]；
– 错误Rring学习（R-LWE）[b-Lyubashevsky]；
– NewHope方案[b-Alkim]。

II.2 基于散列的算法

一些基于散列的算法如下：

– 扩展的Merkle签名方案（XMSS）[b-Buchmann]；
– SPHINCS[b-Bernstein 2015]；
– Leighton-Micali基于散列的签名（LMS）[b-IRTF RFC 8554]

II.3 基于代码的算法

一些基于代码的算法如下：

– 经典McEliece[b-McEliece]；
– Niederreiter方案[b-Dinh]。

II.4 多变量算法

一些基于多元算法的实用签名方案如下：

– Rainbow [b-Ding]；
– 不平衡的oil和vinegar（UOV）[b-Kipnis]。

II.5 后量子加密的NIST标准化

2016 年 12 月 20 日，NIST 宣布了申请公钥后量子密码算法的提名。NIST 第一轮接受了 69 种候选算法，其中包括 20 个数字签名方案和 49 个公钥加密（PKE）或密钥封装机制。2019 年 1 月 30 日，NIST 选择了表 II.1 中列出的 26 种算法作为第二轮候选算法，其中包括九个数字签名方案和 17 个 PKE 以及密钥建立方案[b-NISTIR 8240]。

表II.1 – NIST第二轮算法

分类	问题库	算法
加密/KEM	基于格	Crystals-Kyber
		FrodoKEM
		LAC
		NewHope
		NTRU
		NTRU Prime
		Round 5
		Saber
		Three Bears
	基于代码	Classic McEliece
		NTS-KEM
		BIKE
		HQC
		Rollo
		LEDAcrypt
		RQC
	基于机构	SIKE
签名	基于格	Crystals-Dilithium
		Falcon
		qTesla
	基于多变量	GeMSS
		LUOV
		MQDSS
		Rainbow
	基于散列	Sphincs+
		Picnic

NIST 拟将后量子公钥算法标准化，用于各种协议，如 TLS、安全外壳（SSH）、互联网密钥交换（IKE）、IPsec 和域名系统安全扩展（DNSSEC）[b-NISTIR 8240]。

NIST 从安全性和性能两个角度评估了第二轮算法。NTRU 加密技术发明于 1996 年，几十年来，人们对其安全性已经有了相当好的了解和监督。此外，NTRU 加密在[b-IEEE Std 1363.1]中实现了标准化。经典的 McEliece 是基于未破解的[b-McEliece]，人们认为其具备量子安全性。相比之下，许多其他计划的发布时间不足 10 年。因此，这些方案仍然需密码界开展深入的密码分析，以提高人们对其安全性的信心。特别是起源于[b-Jao]的 SIKE，依赖于寻找超奇异椭圆曲线之间的同源问题。目前此问题的研究水平尚未达到与其他候选方[b-NISTIR 8240]安全问题相同的水准。

完美的前向保密意味着以往的会话密钥不会被披露，即使在长期密钥已经披露的情况下。这是广泛使用的安全协议（如 IPsec 和 TLS）所期望得到的有用的安全属性。在所有候选产品中，只有 SIKE 和 NewHope 能够支持完美的前向保密。

算法的性能是根据公钥、密文和签名的大小以及加密和解密的计算效率加以衡量。与经典的公钥算法相比，PQC 算法通常拥有更大的公钥、密文和签名。根据[b-NIST PQC]，候选的公钥大小从 726 字节到 1 兆字节以上不等。SIKE 的公钥最小，而经典的 McEliece 和 NTS-

KEM 的公钥比其他方案大得多。然而，经典的 McEliece 和 NTS-KEM 可以生成比其他方案更小的密文，其加密速度颇具竞争力。尽管 SIKE 的公钥最小，但其性能似乎比许多其他候选公钥低一个数量级。因此，在选择 PQC 算法时，需要在带宽效率和计算效率之间进行权衡。

2020 年，NIST 计划选择进入最后一轮的最后参选产品，或选择少量候选公钥进行标准化。这意味着标准化的不仅仅是一个，而是一套 PQC 算法。在移动环境中，鉴于空中接口的无线资源宝贵且设备的计算能力有限，因此性能至关重要。IMT-2020 系统应引入最终的标准化算法，这些算法有更小的公钥、密文大小，以及具有竞争力的加密速度。

附录三

量子计算对常用密码算法的影响

（本附录不构成本建议书的组成部分。）

本附录列举了量子计算对常见加密算法的影响。

表III.1总结了大规模量子计算机对常见加密算法的影响，如RSA和高级加密标准（AES）。

目前还不知道这些量子优势能走多远，亦不知经典模型和量子模型可行性之间的差距有多大[b-NISTIR 8105]。

表III.1 – 量子计算机对常用加密算法的影响
[b-NISTIR Quantum report]

加密算法	类型	使用	影响
AES	对称	加密	需要长密钥
SHA-2，SHA-3	散列	散列函数	需要更长的输出
RSA	公钥	签字，密钥传输	不再安全
ECDSA，ECDH	公钥	签字，密钥交换	不再安全
DSA	公钥	签字，密钥交换	不再安全

附录四

量子安全加密码的评估标准

（本附录不构成本建议书的组成部分。）

本附录提供了选择量子安全加密码的NIST评估标准。

提交的加密算法将基于三个方面进行评估：安全性、成本、算法和实施特征[b-NIST-Sub]。

IV.1 安全性

加密方案提供的安全性是评估的最重要因素。方案将根据以下因素进行判断：

公钥加密的应用：后量子算法及其现有的数字签名标准（FIPS 186）和密钥建立标准（SP 800-56A、SP 800-56B）将实现标准化。这些标准用于各种各样的互联网协议，如 TLS、SSH、IKE、IPsec 和 DNSSEC。在评估过程中，方案将根据公钥在这些应用程序中提供的安全性进行评估。如果这种评估对决定哪些算法需要标准化是必要的，则将对所要求应用的实际重要性进行评估。

加密/密钥建立的安全性的定义：针对自适应选择的加密攻击，加密或密钥建立的后量子算法应具备“语义安全性”。该属性在学术文献中通常称为 IND-CCA2 安全性。

上述安全性定义应视作 NIST 关于相关攻击的声明。按照提交者指定的方式使用时，提交的 KEM 和加密方案将根据其提供该属性的表现进行评估。提交者不需提供安全证明，尽管在这种证明可用的情况下会考虑是否加以使用。

为了估算安全强度，可假设攻击者能够访问不超过 2^{64} 个选定密文的解密；然而，亦可考虑涉及更多密文的攻击。

仅短暂加密/密钥建立的安全定义：虽然选择的密文安全对许多现有应用程序是必要的（例如，允许密钥缓存名义上短暂的密钥交换协议），但可以实现一个纯短暂的密钥交换协议，使得加密或 KEM 原语仅需被动安全。

对这些应用而言，针对仅短暂加密/密钥建立的后量子算法，相对于所选纯文本攻击应具有语义的安全性。在学术文献中，该属性通常被标记为 IND-CPA 安全。

按提交者指定的方式使用时，提交的 KEM 和加密方案将根据其提供该属性的表现进行评估。提交者无需提供安全证明，尽管这种证明如果可用的话会被考虑。应充分解释因重复使用密钥而导致的任何安全漏洞。

数字签名的安全定义：数字签名的后量子算法允许针对自适应选择消息攻击，生成存在性不可伪造的数字签名。此属性在学术文献中通常被称为 EUF-CMA 安全。

提交的数字签名算法将根据按提交者指定的使用方式使用时此属性的表现进行评估。

为了估算安全强度，可假设攻击者能够访问不超过 2^{64} 条所选消息的签名。

附加安全属性：虽然前面列出的安全定义涵盖了许多将在评估提交算法时使用的攻击场景，但仍有几个其他属性可取：

安全属性的特性之一就是完美的前向保密。虽然可以通过使用标准加密和签名功能获得该属性，但在某些情况下，这样做的成本可能会高得令人望而却步。特别是，RSA 等具有慢密钥生成算法的公钥加密方案，通常被认为不适合完美的前向保密。在这种情况下，算法的成本和实际安全性之间存在很大的相关性。

安全性和性能相互作用的另一个案例是抵抗旁路攻击。相对于那些在任何抵抗旁路攻击的尝试中性能都会受到严重阻碍的方案，能以最小代价抵抗旁路攻击的方案更受欢迎。我们还注意到，针对旁路攻击的优化实现（例如，恒定时间实现）比不针对边信道攻击的优化实现更有意义。

第三个理想的特性是抵抗多密钥攻击。在理想情况下，攻击者不应通过同时攻击多个密钥获得优势，无论攻击者的目标是攻击单个密钥对，还是攻击大量密钥。

最后一个理想属性是抗误用（虽然定义不明确）。在理想情况下，相关方案不应因孤立的编码错误、随机数生成器故障、随机数复用、密钥复用（仅用于临时加密/密钥建立）等导致灾难性失败。

其他考虑因素：由于公钥密码系统往往包含微妙的数学结构，因此理解数学结构对树立密码系统安全性方面的信心非常重要。为评估这一点，我们将考虑各种因素。在其他条件相同的情况下，简单方案往往比复杂的方案更容易理解。同样，设计原则与知名机构相关研究相关的方案，往往比全新的方案更容易理解，或者相对于通过反复修补旧方案而设计出的方案，更容易受到密码分析的影响。

方案文件的明确度和提交者提供的分析质量应得到考虑。清晰透彻的分析将有助于提高更广泛群体的分析质量和成熟度。提交者提供的任何安全论据或证据都将得到考虑。虽然安全性的证明通常基于未经证实的假设，但这些假设通常可以排除常见的攻击类别，或将新方案的安全性与研究时间更长、更深入的计算问题联系起来。

IV.2 成本

公钥密码系统的成本可以从许多不同的方面加以衡量。

公钥、密文和签名和大小：相关方案将根据产生的公钥、密文和签名大小进行评估。对于带宽受限的应用程序或数据包大小有限的互联网协议，所有上述要点都可能成为重要的考虑因素。公钥大小的重要性可能因应用而异；如果应用程序可以缓存公钥或避免频繁传输公钥，则公钥的大小可能便不那么重要。相比之下，通过在每次会话开始时传输新公钥来寻求获得完美前向保密性的应用程序，可能会从使用相对较小公钥的算法中受益匪浅。

公钥和私钥操作的计算效率：相关方案亦将根据公钥（加密、封装和签名验证）和私钥（解密、解封装和签名）操作的计算效率进行评估。这些操作的计算成本将从硬件和软件两方面评估。公钥和私钥操作的计算成本可能对所有操作都很重要，但有些应用程序或许对其中某一密钥更加敏感。例如，签名或解密操作可以由智能卡等计算受限的设备来完成；或者，负责处理大流量的服务器可能需要花费计算资源的很大一部分验证客户端签名。

密钥生成的计算效率：相关方案还将根据密钥生成操作的计算效率进行评估（如适用）。密钥生成时间重要的最常见情况是使用公钥加密算法或KEM提供完美的前向保密性。尽管如此，但在某些应用中，密钥生成时间对于数字签名方案可能也很重要。

解密失败：一些公钥加密算法和KEM，即使正确实现，偶尔也会产生无法解密/解封的密文。对于大多数应用，这种解密失败很少或根本不存在至关重要。对于解密/解封装失败的算法，提交者必须提供失败率，以及针对这些失败可能导致的安全影响的分析。虽然应用程序总可通过多次加密相同的明文获得可接受的低解密失败率，并且交互式协议可在密钥建立失败时简单重启，但这些类型的解决方案亦有其自身的性能成本。

IV.3 算法和实现的特点

灵活性：假设整体安全性和性能良好，灵活性较大的方案比灵活性较小的方案更能满足较多用户的需求，因此更加可取。

“灵活性”的一些示例可能包括（但不限于）以下内容：

1) 可通过修改该方案提供超出公钥加密、KEM（密钥封装机制）或数字签名（例如，异步或隐式认证的密钥交换等）的最低要求附加功能。
2) 定制方案参数以满足一系列安全目标和性能目标是一项直截了当的工作。
3) 这些算法可以在各种平台上安全高效地实现，包括智能卡等受约束的环境。
4) 算法的实现可以并行操作，以获得更高的性能。
5) 该方案可以结合至现有的协议和应用，只需要尽可能少的改变。

简单性：相关方案将根据其设计的相对简单性加以判断。

使用：在评估过程中将考虑可能阻碍或促进算法或算法实现的广泛因素，其中包括但不限于涵盖算法或其实现的知识产权问题以及相关方许可的可用性和条款。评估方将考虑提交者和任何专利所有人在声明中所做保证，并强烈倾向于承诺在合理的条款以及没有明显不公平歧视的情况下，无偿提供许可。

参考资料

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦