5G网络量子安全算法应用研究

王聪丽[1,2]，李金慧[1,2]，王靖然[1,2]，薛伟佳[1,2]，王锦华[1,2]，王骞然[1,2]
（1. 中国电信股份有限公司研究院，上海 201315；
2. 云网基础设施安全国家工程研究中心，上海 201315）

摘　要：随着5G网络的广泛应用，数据传输速度与容量显著提升，推动了物联网、自动驾驶、远程医疗等领域的创新发展，同时也对网络安全提出了更高要求。量子计算的进步对传统公钥密码体系构成重大威胁，Shor算法和Grover算法可分别破解基于大整数分解和离散对数问题的公钥密码，并提高对称加密算法和杂凑算法的破解效率。为应对这一挑战，全球多个标准化组织正积极推进量子安全密码的研究与标准化工作。首先概述了5G网络架构及其安全需求，并分析了量子计算对传统密码体系的影响。随后，介绍了量子安全密码算法的最新进展，并探讨了这些算法在5G网络终端接入与数据传输安全中的集成方式。最后，提出了量子安全密码应用策略，并验证了其技术可行性，以期为构建更加安全可靠的5G网络提供理论和技术参考。

关键词：5G网络；量子安全算法；网络安全；密码应用
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024231

Research on the application of quantum-secure algorithms in 5G network

WANG Congli[1,2], LI Jinhui[1,2], WANG Jingran[1,2], XUE Weijia[1,2], WANG Jinhua[1,2], WANG Qianran[1,2]
1. China Telecom Research Institute, Shanghai 201315, China
2. National Engineering Research Center of Cloud and Network Infrastructure Security, Shanghai 201315, China

Abstract: With the widespread application of 5G networks, data transmission speed and capacity have been significantly improved, promoting innovative development in fields such as the Internet of things, autonomous driving, and telemedicine. At the same time, higher requirements are put forward for network security. The progress of quantum computing technology poses a major threat to the traditional public key cryptosystem. Shor's algorithm and Grover's algorithm can crack public key cryptography based on the holeyer factorization and discrete logarithm problems respectively, and improve the cracking efficiency of symmetric cryptography and hash algorithms. To address this challenge, multiple global standardization organizations are actively promoting the research and standardization of quantum-secure cryptography. Firstly, the 5G network architecture and its security requirements were outlined, and the impact of quantum computing on traditional cryptography was analyzed. Subsequently, the latest progress of quantum-secure cryptography algorithms was introduced, and the integration methods of these algorithms in 5G net-

收稿日期：2024−08−09；**修回日期：**2024−09−23
基金项目：国家重点研发计划项目（No.2022YFB2902100）
Foundation Item: The National Key Research and Development Program of China (No.2022YFB2902100)

work terminal access and data transmission security were discussed. Finally, a quantum-secure cryptography application strategy was proposed and its technical feasibility was verified, in order to provide theoretical and technical references for building a more secure and reliable 5G network.

Key words: 5G network, quantum-safe algorithm, network security, cryptographic application

0 引言

随着5G网络的普及与应用，数据传输速率与容量达到新高度，推动了物联网、自动驾驶、远程医疗等领域的创新发展，同时也对网络安全提出更高要求。国内外标准化组织持续推进密码技术在5G网络中的应用，以满足终端接入安全、用户身份隐私保护、信令和数据传输的机密性与完整性保护等需求，防范用户设备、接入网、核心网、软硬件基础设施等方面的网络安全风险。

近几年，全球主要国家及科技巨头在量子计算机领域的研发投入持续增加，使得量子计算机的性能持续优化并取得突破性进展。量子计算机通过运行Shor算法[1]可在多项式时间内破解基于大整数分解和离散对数问题的公钥密码，如RSA、Diffie-Hellman、ECDH、ECDSA及相关安全协议、产品或系统；通过运行Grover算法[2]可提高破解对称加密算法和杂凑算法的效率，使对称加密算法安全性减半，杂凑算法安全性降为原来的2/3，如AES、ZUC及SHA系列算法。因此，一旦量子计算机实现实用化，现有加密算法将面临被破解的风险。

为应对这一挑战，全球多个标准化组织正积极开展量子安全密码研究并制定系列标准。美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）于2016年12月启动后量子密码学（post quantum cryptography，PQC）标准化项目[3]，历经近8年，在2024年8月13日发布首批3个PQC算法标准[4]。国际互联网工程任务组（Internet Engineering Task Force，IETF）启动传输层安全（transport layer security，TLS）协议、IP安全（IP security，IPSec）协议等互联网协议修订，并于2023年1月成立后量子协议使用（Post-Quantum Use in Internet Protocol，PQUIP）工作组，以推进PQC在互联网协议中的应用与工程实践[5]。欧洲电信标准组织（European Telecommunications Standards Institute，ETSI）成立量子安全密码组，旨在推动量子安全密码标准的全球适应性与兼容性，并提供技术规范、实施指南及工具[6]。国际标准化组织/国际电工委员会第一联合技术委员会（ISO/IEC JTC1）信息安全工作组（SC27）于2020年5月发布后量子密码学综述[7]，并于2024年6月发布有状态的基于杂凑的签名机制标准，积极推进PQC标准化工作[8]。此外，ISO/IEC JTC1启动了对现有公钥加密标准ISO /IEC 18033-2: 2006 /WD Amd 2的增补工作[7]。第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）自2018年起对5G系统的后量子迁移展开研究[9]，评估量子计算威胁及对策，并在2022—2024年的Release19阶段通过多项加密算法升级的课题立项[10-12]。然而，现有研究主要集中在量子安全算法标准化、互联网安全协议升级、量子计算对5G网络密钥管理及传统密码算法的影响等方面，在5G网络量子安全算法应用的系统性分析上存在不足。

综上所述，量子计算技术的发展使现有加密算法面临被破解的风险，促使5G网络采用量子安全算法以增强安全性。因此，开展5G网络量子安全算法应用的系统性分析具有重要意义。本文首先介绍5G网络架构及其接口，归纳量子计算对现有密码学的冲击，并分析5G网络面临的安全风险。基于此，提出相应的量子安全算法应

用策略，为5G网络的量子安全密码应用提供参考。

1　5G网络架构及安全需求

5G作为新一代无线通信技术，是实现万物互联的关键新型基础设施，其架构主要包括3个部分：5G核心网（5G core network，5GC）、无线电接入网（radio access network，RAN）及用户设备（user equipment，UE）[13-14]。5GC作为5G网络的控制中心，负责数据传输、网络管理和服务功能，由控制面与用户面组成，并通过服务化架构及网络功能虚拟化（network functions virtualization，NFV）技术实现灵活高效的服务部署。RAN主要由5G基站（the next generation node B，gNB）构成，负责无线信号的发送与接收。用户设备包括智能手机、平板电脑等设备，通过5G新空口（new radio，NR）接口与RAN相连，以获取高速、低延迟、可靠的通信服务。

在非漫游场景下，基于服务化接口的5G非漫游系统架构[15]如图1所示。5GC由下列网络功能（network function，NF）组成：接入和移动性管理功能（access and mobility management function，AMF）、会话管理功能（session management function，SMF）、用户平面功能（user plane function，UPF）、统一数据管理（unified data management，UDM）、认证服务器功能（authentication server function，AUSF）、网络存储功能（network repository function，NRF）、网络切片选择功能（network slice selection function，NSSF）、网络开放功能（network exposure function，NEF）、策略控制功能（policy control function，PCF）、应用功能（application function，AF）。5GC的主要接口包括N1、N2、N3、N4、N6、N9参考点及服务化接口（service based interface，SBI），具体如下。

（1）N1接口是UE与AMF之间的逻辑接口，实际经由gNB透传，主要传输UE和5GC之间的非接入层（non access stratum，NAS）信令，包括UE注册、连接管理、移动性管理等相关的控制信息。

（2）N2接口是RAN与AMF之间的控制面接口，支持UE上下文管理、移动性管理和协议数据单元（protocol data unit，PDU）会话管理等功能，用户面采用基于IP的NG-AP协议。

（3）N3接口是RAN与UPF之间的用户面接口，承载用户数据流，用户面采用基于UDP/IP的GTP-U协议。

（4）N4接口是SMF与UPF之间的接口，用于会话建立、修改和释放，以及策略规则的应用，其控制面协议采用基于TCP/IP的PFCP协议，用户面采用基于UDP/IP的GTP-U协议。

（5）N6接口是UPF与外部数据网络（data

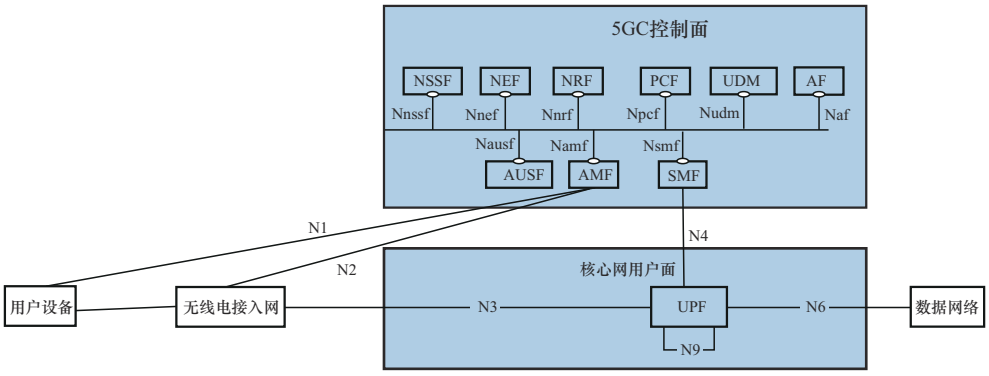

图1　基于服务化接口的5G非漫游系统架构

network，DN）之间的接口，允许用户设备访问外部网络服务，主要是一个用户面接口，无特定控制面协议栈，控制面操作通过其他接口（如N4）完成，用户面采用基于TCP/IP或UDP/IP协议。

（6）N9接口是两个UPF实例之间的用户面接口，支持UPF之间的数据转发，用户面采用基于UDP/IP的GTP-U协议。

（7）5GC中网络功能之间的控制面接口采用SBI，包括Namf、Nsmf、Nudm、Nnrf、Nnssf、Nausf、Nnef、Naf、Npcf。SBI协议栈如图2所示，使用HTTP/2协议实现NF间的交互。所有NF必须支持TLS协议，以提供传输层的安全保护[16]。

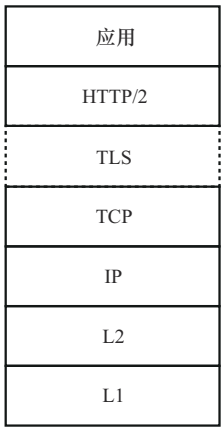

图2　SBI协议栈

5G NR协议栈如图3所示，分为用户面和控制面。用户面负责用户数据传输，包括物理（physical，PHY）层、媒体接入控制（medium access control，MAC）层、无线链路控制（radio link control，RLC）层、分组数据汇聚协议（packet data convergence protocol，PDCP）层、服务数据调整协议（service data adaptation protocol，SDAP）层。控制面负责系统信令处理，依次为PHY层、MAC层、RLC层、PDCP层、无线资源控制（radio resource control，RRC）层和NAS层[17]。

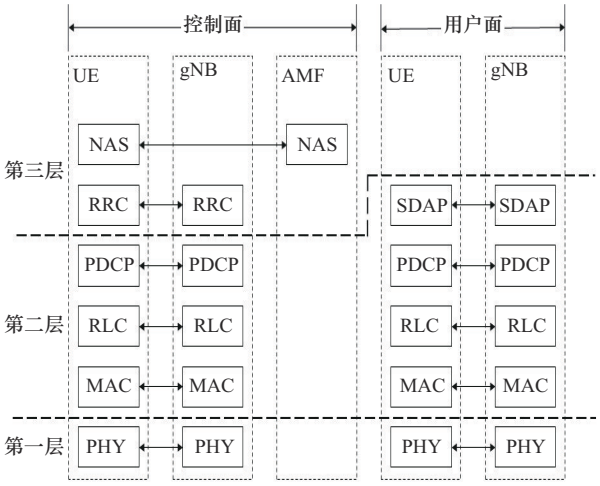

图3　5G NR协议栈

由于5G接入网空口信道的开放性与核心网的复杂性，用户设备易受伪基站攻击，5G网络亦面临非授权恶意终端接入所致的网络瘫痪、隐私泄露及数据篡改等安全威胁，因此，5G网络需要有效的身份验证机制，以实现网络与终端的双向鉴权认证，确保接入终端的合法性。同时，需要对永久用户标识进行加密，以保障用户隐私。此外，还应加强数据机密性和完整性保护，利用加密算法将明文转换为密文，并通过完整性算法检测信令消息和用户面数据的真实性与完整性。

2　量子计算对传统密码体系的威胁与应对策略

量子计算作为遵循量子力学原理的新型计算模式，具有远超经典计算的强大并行计算能力，在密码破解领域应用潜力巨大。尽管量子计算机的实用化进程仍在推进，但自2019年谷歌“悬铃木”实现量子优越性以来，全球在超导、光量子、离子阱和硅基半导体等技术路线上取得显著进展。同时，随着Shor、Grover等典型量子算法的提出与优化，相关运算操作的时间复杂度可从指数级别降至多项式级别，使得传统加密技术面临的破解风险显著上升。因此，需要构建并完善量子安全的密码体系作为应对策略。

2.1　量子计算对传统密码体系的威胁

当前广泛应用的密码体系分为对称加密算法、杂凑算法、公钥密码这3类。

对称加密算法和杂凑算法的安全性目前主要受Grover量子搜索算法的影响。Grover算法能够实现对无结构化数据库搜索效率的二次加速，从而提升密码破解效率，降低密码算法安全性。运用Grover算法，对称加密算法的时间复杂度由经典计算机的O（2^n）降低为量子计算机的O（$2^{n/2}$），杂凑算法的时间复杂度由经典计算机的O（$2^{n/2}$）降低为量子计算机的O（$2^{n/3}$）[18-19]。

公钥密码的安全性建立在特定数学困难问题的计算复杂度之上。例如，RSA算法依赖于大整数分解问题，ECC和Diffie-Hellman则依赖于离散对数问题。这些算法的安全性源于经典计算机在合理的时间内难以解决相应问题。然而，Shor量子算法能够在多项式时间内破解大整数分解和离散对数问题，这意味着具备运行Shor算法能力的量子计算机将能够破解传统公钥密码。

常用的各类密码算法在经典计算环境和量子计算环境的安全强度对比[20]见表1。

由表1可知，Grover算法将对称加密的安全性降低至原水平的50%；杂凑算法的安全性降低至原水平的2/3；Shor算法使得基于大整数分解和离散对数问题的公钥密码失去安全性。依据NIST、欧盟委员会及信息安全领域的专业共识，应逐步采用在经典计算环境与量子计算环境下均能达到112 bit安全强度的量子安全算法[21-22]，以满足未来计算环境下对高安全性的需求，抵御量子计算引发的安全威胁。

2.2　量子安全的密码体系构建策略

2.2.1　对称加密算法与杂凑算法

量子计算对传统对称加密算法和杂凑算法的影响较为有限，可通过增大算法参数予以弥补，亦可设计新的抗量子计算对称加密算法与杂凑算法。但需要注意的是，新算法的安全性需要历经长时间的同行评审和实际应用测试。例如，可将对称加密算法AES-128、SNOW 3G、ZUC-128升级为AES-256、SNOW-V[23]、ZUC-256，将杂凑算法SHA-256升级为SHA2-512[24]或SHA3-512[25]。

2.2.2　非对称加密算法

PQC是专为抵御量子计算攻击而设计的非对称加密技术，其安全性依托于特定的数学难题。基于格的方法在学术研究、标准制定及实际应用

表1　常用的各类密码算法在经典计算环境和量子计算环境的安全强度对比

密码体制	密码算法	密钥/摘要长度/bit	安全强度/bit		受到量子计算的影响
			经典计算环境	量子计算环境	
对称加密算法	AES-128	128	128	64	Grover算法：安全性减半
	ZUC-128	128	128	64	
	SNOW 3G	128	128	64	
	AES-256	256	256	128	
	ZUC-256	256	256	128	
	SNOW-V	256	256	128	
杂凑算法	SHA-256	256	128	80	Grover算法：安全性降低为2/3
	SHA-512	512	256	192	
公钥密码	RSA2048	2 048	112	0	Shor算法：不再安全
	ECC-256	256	128	0	
	ECC-384	384	192	0	

中的表现尤为突出。

在国外，NIST主导了PQC算法的标准化工作。NIST于2024年8月13日正式发布3项算法标准，分别是用于密钥交换的模块化格基密钥封装机制标准（ML-KEM）[26]、用于数字签名的模块化格基数字签名标准（ML-DSA）[27]与无状态哈希数字签名标准（SLH-DSA）[28]。NIST发布的3个标准化算法见表2。

在我国，PQC算法研究呈现蓬勃发展态势。以清华大学、中国科学院信息工程研究所、上海交通大学、复旦大学及密码科学技术全国重点实验室为代表的多家高校与科研机构，在2018年由中国密码学会主办的第四届全国密码算法设计竞赛中表现出色[29]，并深度参与NIST和ISO等国际组织的标准制定工作，有效提升了我国在PQC领域的国际影响力和技术创新能力。当前，我国正在加速推进基于杂凑函数的抗量子数字签名技术的标准化工作。基于国产杂凑函数SM3的LMS和HSS[27]标准制定项目，在2023年年底获得国家密码管理局下属密码行业标准化技术委员会的正式立项。

综上所述，当量子计算机达到足够性能时，传统的公钥密码算法将不再安全，对称加密算法和杂凑算法也将面临安全强度不足的问题。因此，构建具备抗量子计算攻击能力的密码体系变得至关重要。量子安全密码体系可用于数据加密、数据完整性保护、密钥交换以及数字签名，已成为国内外学术研究、标准制定和实际应用的重点方向。通过部署这些新型算法，能够保障网络和信息系统在量子时代依然保持高度的安全性。

3 量子安全密码体系在5G网络中的应用

在5G网络中，传统密码算法在多个关键环节得到应用[28]，包括终端接入时的身份隐私保护、主认证、密钥派生及空口安全，数据传输时不同安全域间使用的IPSec协议、同一安全域内使用的TLS协议以及5G核心网内的公钥基础设施。鉴于量子计算对未来网络安全的潜在影响，上述环节需要逐步迁移至量子安全算法。下面将从5G网络密码应用现状与量子安全密码应用建议两个方面展开探讨，详细总结见表3。

3.1 终端接入安全

3.1.1 用户身份隐私保护

UE首次接入网络时，使用椭圆曲线集成加密方案（elliptic curve integrated encryption scheme，ECIES）加密签约用户永久标识符（subscription permanent identifier，SUPI），从而生成签约用户隐藏标识符（subscription concealed identifier，SUCI），以保护用户隐私。其原理是UE和5G网络使用各自的私钥和对方的公钥，通过椭圆曲线迪菲－赫尔曼（elliptic curve Diffie-Hellman，ECDH）机制协商出一个共享密钥，然后使用基

表2 NIST发布的3个标准化算法

标准名称	名称缩写	标准编号	标准化前的算法名称	算法类型	算法用途	现有算法对标	优先级
模块化格基密钥封装机制标准	ML-KEM	FIPS 203	CRYSTALS-Kyber	公钥加密/密钥封装	通信双方在公共信道上安全地建立共享密钥	RSA、DH、ECDH、SM2	推荐标准
模块化格基数字签名标准	ML-DSA	FIPS 204	CRYSTALS-Dilithium	数字签名	身份鉴别、数据完整性保护	RSA、ECDSA、SM2	推荐标准
无状态哈希数字签名标准	SLH-DSA	FIPS 205	Sphincs+	数字签名	身份鉴别、数据完整性保护	RSA、ECDSA、SM2	备用标准

表3　5G网络量子安全密码算法应用参考

场景	功能	涉及资产	现有密码算法/协议	3GPP密码套件	需求	量子安全密码应用建议
终端接入安全	用户身份隐私保护	UE UDM	ECIES	密钥协商：ECDH 密钥派生：ANSI-X9.63-KDF 杂凑算法：SHA-256 机密性保护：AES-128 完整性保护：HMAC-SHA-256	密钥协商协议需要进行更换； 机密性保护算法的密钥长度需要增加	密钥协商协议选用量子安全密码套件； 机密性保护算法升级为AES-256
	主认证	UE UDM	Milenage算法集 TUAK算法集	Milenage：基于对称加密算法AES-128或AES-256的f1、 f1*、f2、f3、f4、f5、f5*、f5**函数 TUAK：基于杂凑算法Keccak-128或Keccak-256的f1、f1*、f2、f3、f4、f5 、f5*函数	对称加密算法的密钥长度需要增加； 杂凑算法的摘要长度需要增加	Milenage协议升级； TUAK协议升级
	密钥派生	ME gNB AMF SEAF AUSF N3IWF	根密钥长度：128 bit或256 bit 密钥派生函数：GKDF 杂凑算法：HMAC-SHA-256		根密钥长度需要增加； 派生出的密钥长度需要增加	根密钥长度升级为256 bit； 不再截断GKDF的输出长度
	空口安全	UE gNB AMF	机密性保护：SNOW 3G、AES-128、ZUC-128 完整性保护：SNOW 3G、AES-128、ZUC-128		机密性保护算法的密钥长度需要增加； 完整性保护算法的密钥长度需要增加	机密性保护算法升级为SNOW-V、AES-256、ZUC-256； 完整性保护算法升级为SNOW-V、AES-256、ZUC-256
数据传输安全	域间安全通信	N2、N3、N4、N6、N9接口	IPSec	加密算法：ENCR_AES_CBC ENCR_AES_CCM_8 ENCR_AES_GCM_16 ENCR_CHACHA20_POLY1305 ESP和AH的认证算法：AUTH_AES_128_GMAC; AUTH_AES256_GMAC; AUTH_HMAC SHA2_256_128; AUTH_HMAC_SHA2_512_256;	传统公钥密码算法需要进行更换； 对称加密算法的密钥长度需要增加； 杂凑算法的摘要长度需要增加	选用量子安全密码套件
	域内安全通信	核心网网元	TLS	TLS1.2： TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256； TLS_DHE_RSA_WITH_AES_128_GCM_SHA256； TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384； TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS1.3： TLS_AES_128_GCM_SHA256； TLS_AES_256_GCM_SHA384； TLS_CHACHA20_POLY1305_SHA256； TLS_AES_128_CCM_SHA256； TLS_AES_128_CCM_8_SHA256		
	公钥基础设施	PKI公钥基础设施		公钥密码算法：RSA、ECDSA 杂凑算法：SHA-256、SHA-384	传统公钥密码算法需要进行更换	选用后量子密码算法

于SHA-256的ANSI-X9.63-KDF函数派生出机密性密钥和完整性保护密钥。最后，使用AES-128算法基于机密性密钥对SUPI进行加解密，使用HMAC-SHA-256算法基于完整性密钥对SUCI进行完整性保护和验证。

为了在量子时代有效保障用户身份隐私，建议采取以下措施：（1）采用标准化的PQC密钥交换算法，如ML-KEM，替代现有的ECDH机制来生成共享密钥；（2）升级密钥派生函数，利用SHA3-512等更强大的杂凑算法来增加ANSI-X9.63-KDF摘要的长度；（3）推荐使用256位密钥长度的量子安全对称加密算法，如AES-256，以增强SUPI的机密性保护。

3.1.2 主认证

UE接入5G网络时，采用5G-AKA或EAP-AKA协议进行相互认证。目前，这两个协议均支持两种算法集：一种基于Milenage[30-33]算法集，采用AES算法进行认证向量的生成和响应；另一种基于TUAK[34]算法集，采用Keccak算法进行认证向量的生成和响应。

根据当前的3GPP Release 19标准，Milenage和TUAK算法集均支持128 bit和256 bit的密钥输入。本文建议网络运营商和设备制造商优先使用256 bit密钥，并采用AES-256或Keccak-256算法来生成认证向量及身份认证响应。

3.1.3 密钥派生算法

UE和5GC共享长期密钥K，该密钥长度为128 bit或256 bit，分别存储于USIM卡和UDM/ARPF中。5G系统中的密钥层次推衍如图4所示，从K派生出CK和IK，进而派生出K_{AUSF}、K_{SEAF}、K_{AMF}、K_{NASint}、K_{NASenc}、K_{N3IWF}、K_{gNB}、K_{RRCint}、K_{RRCenc}、K_{UPint}和K_{UPenc}等。所有派生过程均采用基于HMAC-SHA-256的GKDF函数，并最终截取K_{RRCint}、K_{RRCenc}、K_{UPint}、K_{UPenc}、K_{NASint}和K_{NASenc}的前128 bit，用于空口数据的机密性和完整性保护。

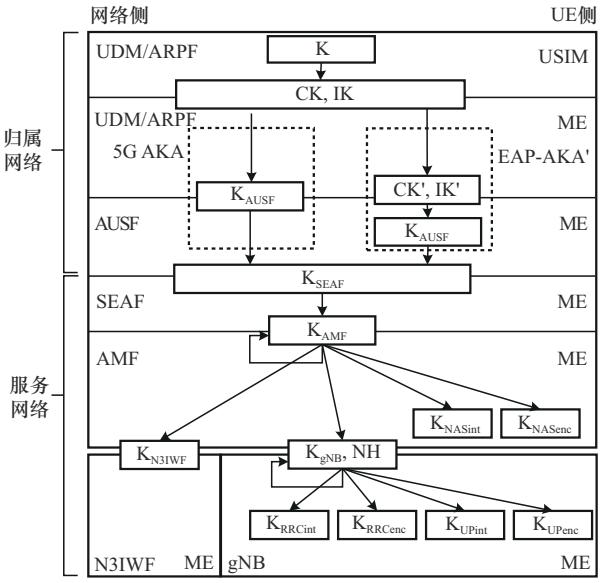

图4 5G系统中的密钥层次推衍

当前，业内普遍采用128 bit的根密钥K。然而，在量子计算环境中，128 bit密钥的有效安全强度会降至64 bit，从而削弱了主密钥及其派生密钥的安全性。为生成具有256 bit熵的会话密钥，建议采取以下措施：（1）将根密钥K的长度增加至256 bit；（2）避免对GKDF生成的256 bit输出执行截断操作。

3.1.4 空口安全算法

UE与gNB之间的Uu接口用于传输RRC信令和用户面数据。UE与AMF之间的N1接口主要传输NAS信令。对Uu接口和N1接口上传输的信令和数据的机密性与完整性保护主要采用AES-128、SNOW 3G、ZUC-128这3种密码算法。5G协议支持的机密性保护算法和完整性保护算法分别见表4、表5。

本文建议网络运营商和设备制造商将空口安全算法升级为具有256 bit密钥长度的量子安全对称加密算法，如将AES-128、Snow 3G、ZUC-128升级为AES-256、Snow-V、ZUC-256。

3.2 数据传输安全

对于5G网络域间安全通信、域内安全通信及公钥基础设施，3GPP国际标准仅规定了安全

表4　5G协议支持的机密性保护算法

算法标识	机密性算法	保护内容
128-NEA0	空加密算法	不进行机密性保护
128-NEA1	SNOW 3G算法	使用K_{NASenc}密钥和SNOW 3G算法，保护N1接口NAS信令的机密性
128-NEA2	AES-128算法	使用K_{UPenc}密钥和AES-128算法，保护Uu接口用户面数据的机密性
128-NEA3	ZUC-128算法	使用K_{RRCenc}密钥和ZUC-128算法，保护Uu接口RRC信令的机密性

表5　5G协议支持的完整性保护算法

算法标识	完整性算法	保护内容
128-NIA0	空加密算法	不进行完整性保护
128-NIA1	SNOW 3G算法	使用K_{NASint}密钥和SNOW 3G算法，保护N1接口NAS信令的完整性
128-NIA2	AES-128算法	使用K_{UPint}密钥和AES-128算法，保护Uu接口用户面数据的完整性
128-NIA3	ZUC-128算法	使用K_{RRCint}密钥和ZUC-128算法，保护Uu接口RRC信令的完整性

协议，而未定义具体的密码算法。在实际应用中，通常由各厂商自行选择合适的密码套件以实现安全通信。

3.2.1　域间安全通信

在5G网络架构中，N2、N3、N4、N6和N9接口位于不同安全域之间，通常采用基于IP协议的应用层通信协议，实现基站与核心网、核心网控制面与用户面、不同核心网用户面之间以及核心网与数据网络的连接。这些接口的数据传输安全由IPSec协议保障，IPSec协议通常使用DH算法或非对称加密技术进行密钥协商。

3.2.2　域内安全通信

5GC控制面采用服务化架构（service based architecture，SBA），网元间通过基于HTTP的SBI进行通信，并使用TLS协议保障接口安全。网元间的授权和访问控制采用OAuth协议，OAuth令牌的分发通过TLS协议加密的通道完成。TLS协议使用ECDHE或DHE进行密钥协商。

根据上述分析，域间安全通信依赖于IPSec协议，域内安全通信依赖于TLS协议。尽管这两类协议工作在不同的网络层级，但均涉及两个关键环节：一是通过身份认证和密钥协商过程生成会话密钥。在这一步骤中，可借助两种主流方法完成身份认证，分别是预共享对称密钥和基于公钥的方法，后者通常结合数字证书使用。二是在数据安全传输环节，利用生成的会话密钥，通过对称加密算法来保障数据传输的机密性和完整性。

针对量子安全性需求，在身份认证和密钥协商环节，若采用预共享密钥方法，建议使用256 bit的预共享对称密钥，并结合量子安全的密钥派生函数生成会话密钥；若采用基于数字证书的方法，则建议在数字证书中集成量子安全的非对称加密算法，并使用量子安全的密钥协商协议生成会话密钥。在数据安全传输环节，建议使用具有256 bit密钥的对称加密算法来保护传输数据的机密性和完整性。

3.2.3　公钥基础设施

3GPP TS 33.310[35]定义了移动通信网络域安全认证框架，引入了基于PKI/CA的安全机制，以支持使用NDS/IP或者TLS协议的网元进行身份认证。网元设备出厂时由供应商预装数字证书，作为初次接入运营商网络的身份凭据，经网管/网关验证通过后方可接入业务网络。设备接入运营商网络后，需要由运营商的CA颁发新的证书用于业务连接，例如，设备与网管之间的OM TLS连接、基站与核心网之间的数据平面IPSec

连接。数字证书的全生命周期管理遵循证书管理协议（certificate management protocol version 2，CMPv2）[36-38]，该协议通常结合加密、数字签名、消息鉴别码或密钥管理协议保障数据机密性和完整性。

数字证书格式遵循X.509国际标准与相应的国内标准。在数字证书中集成量子安全密码算法，可通过以下两种方式实现：（1）直接将数字证书中的传统密码算法替换为量子安全密码算法；（2）采用混合证书模式，在同一数字证书中同时包含传统密码算法和PQC算法[39-42]。此外，建议在CMPv2协议的消息交互过程中使用量子安全算法，以保障CMP消息传输的安全性。

3.3 可行性分析

5G网络中的ECIES协议、Milenage/TUAK算法集、机密性/完整性保护算法以及TLS/IPSec协议，均基于对称加密算法或公钥密码算法实现。针对这些底层算法设计实验方案，论证上述应用方法的可行性。对于AES对称加密算法，在配置32 GB内存、第12代Intel® Core™ i5-12600KF处理器（3.70 GHz）且运行Ubuntu 20.04.4 LTS系统的环境下，使用OpenSSL（3.3.2版本），利用“OpenSSL speed (algorithm)”命令对各算法执行20 s性能测试，评估平均时延。在相同软硬件环境中，对RSA-2048、ECDSA（包括ED25519与NIST P-256）等传统公钥密码算法进行测试。对于Kyber、Dilithium等后量子公钥密码算法，聚焦NIST发布的标准化算法，对其官方参考实现进行性能对比分析。具体测试结果见表6、表7。

密码算法的性能受软硬件运行环境的影响较大，而5G网络对密码算法的具体性能要求并非固定不变，需要根据应用场景、网络负载及设备能力综合考虑。根据表7数据，量子安全公钥密码算法的私钥、公钥、密文和签名大小显著大于传统算法，可能导致消息整体尺寸增加。例如，量子安全算法的公钥大小在64～2 592 byte，而传统算法的公钥大小则在32～256 byte。Dilithium设计简单，部署更方便，适用于大部分应用场景。Sphincs+密钥生成与验证速度较快，但劣势是数字签名速度较慢，签名巨大，应用较复杂。Falcon带宽需求最小，且验签速度很快，签名尺寸相对最小，但劣势是在受限环境中密钥生成困难。对于量子安全对称加密算法，5G的下行链路数据速率最高可达到20 Gbit/s，如URCCL场景要求极低的时延和高带宽，规定了1 ms的端到端延迟，AES-256-CTR可达到该要求。此外，OpenSSL密码库尚未支持ZUC-256、SNOW-V算法。目前已知ETSI SAGE已向3GPP提交了AES-256、SNOW-V、ZUC-256的评估结果，3GPP正计划增加支持256 bit对称加密算法的标准及相关测试数据[43]。

总体而言，鉴于无线带宽的稀缺性和设备计算能力的限制，为在5G网络中实现有效应用，可选择密钥更小、加密操作速度更快的量子安全算法，并在后续标准制定过程中充分考虑算法的安全性、参数大小和加密速度对5G网络的影响，选择均衡适合的算法套件。

表6 对称加密算法加密性能对比

算法	不同明文长度对应的加密性能/（Gbit·s^{-1}）						
	64 byte	256 byte	1 024 byte	2 048 byte	4 096 byte	8 192 byte	16 384 byte
AES-128-CBC	17.134	17.521	17.622	17.631	17.642	17.650	17.652
AES-128-CTR	35.390	68.520	91.750	96.770	99.400	100.840	101.400
AES-256-CBC	12.662	12.866	12.928	12.935	12.940	12.943	12.945
AES-256-CTR	29.510	57.810	71.200	74.010	75.790	76.310	76.610

表7　公钥密码算法性能对比

算法类型	算法名称	安全级别	平台	私钥长度/byte	公钥长度/byte	密文/签名长度/byte	密钥生成速度/clock cycle	加密/签名速度/clock cycle	解密/验签速度/clock cycle
公钥加密/密钥封装	Kyber512	Level-1	Intel Core-i7 4770K (Haswell) CPU	1 632	800	768	1.23×10^5	1.55×10^5	1.88×10^5
	Kyber768	Level-3		2 400	1 184	1 088	1.99×10^5	2.35×10^5	2.75×10^5
	Kyber1024	Level-5		3 168	1 568	1 568	3.07×10^5	3.47×10^5	3.97×10^5
数字签名	Falcon-512	Level-1	Intel® Core® i5-8259U at 2.3 GHz, TurboBoost disabled	7 553	897	666	$1.987\ 2\times10^7$	$3.866\ 78\times10^5$	8.234×10^4
	Falcon-1024	Level-5		13 953	1 793	1 280	$6.313\ 5\times10^7$	$7.895\ 64\times10^5$	$1.684\ 98\times10^5$
	SPHINCS+ (SHA-256)- 128f	Level-1	3.1 GHz Intel Xeon E3-1220 CPU (Haswell)	64	32	17 088	$5.590\ 602\times10^6$	$1.386\ 105\times10^8$	$7.757\ 942\times10^6$
	SPHINCS+ (SHA-256)- 192f	Level 3		96	48	35 664	$8.227\ 944\times10^6$	$2.329\ 738\ 8\times10^8$	$1.176\ 838\ 2\times10^7$
	SPHINCS+ (SHA-256)- 256f	Lever-5		128	64	49 856	$2.176\ 359\times10^7$	$4.68\ 188\ 036\times10^8$	$1.193\ 416\ 4\times10^7$
	Dilithium2	Level-2	Intel Core-i7 6600U (Skylake) CPU	2 528	1 312	2 420	3.01×10^5	1.355×10^6	3.27×10^5
	Dilithium3	Level-3		4 000	1 952	3 293	5.44×10^5	2.349×10^6	5.22×10^5
	Dilithium5	Level-5		4 864	2 592	4 595	8.19×10^5	2.857×10^6	8.72×10^5
	NIST P-256	Level-1	Intel Core-i5-12600KF @ 3.7 GHz	32	32	64	*	7.3×10^4	2.33×10^5
	ED25519	Level-1		32	32	64	*	5.4×10^4	1.73×10^5
	RSA2048	Level-2		256	256	256	$1.031\ 67\times10^8$	1.441×10^6	4.4×10^4
公钥加密/密钥封装	RSA2048	Level-2		256	256	256	$1.093\ 64\times10^8$	4.5×10^4	1.458×10^6

注：*表示OpenSSL speed test不包含密钥生成测试。

4　结束语

5G网络的安全机制旨在保护无线接入网和核心网的数据机密性与完整性。当前，AES、SNOW 3G和ZUC算法采用128 bit密钥长度，符合网络安全标准；TLS和IPSec协议采用传统密码套件，同样满足安全需求。然而，量子计算的发展可能削弱现有密码算法的安全性。预计未来的5G版本将增强这些算法。3GPP正在推进在5G网络中支持256 bit对称加密算法的研究，IETF等标准化组织也在推进PQC应用标准的制定，并发布了支持PQC算法的TLS 1.3、IKEv2和X.509标准草案。

本文建议，5G网络中的TLS和IPSec协议应更新其算法套件，逐步采用量子安全密码套件。同时，5G网络中的对称加密算法应支持并适时过渡到256 bit密钥。在引入新算法时，应全面评估密钥长度、密文长度和计算速度，以确保新算法在安全性和效率方面均能满足5G网络的实际需求。此外，建议推动国产PQC算法的研发和标准化工作，以提高我国在网络安全领域的核心竞争力，为5G网络及数字经济发展提供坚实的安全保障。

参考文献：

[1] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124–134.

[2] GROVER K L. A fast quantum mechanical algorithm for database search[C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC ’96). New York: ACM Press, 1996: 212-219.

[3] NIST. NIST asks public to help future-proof electronic information[EB]. 2016.

[4] NIST. NIST releases first 3 finalized post-quantum encryption standards[EB]. 2024.

[5] IETF. Post-Quantum use in protocols (pquip)[EB]. 2023.
[6] ETST. Quantum-Safe cryptography (QSC)[EB]. 2020.
[7] 赖俊森, 赵文玉, 张海懿, 等. 量子计算信息安全威胁与应对策略分析[J]. 信息通信技术与政策, 2024, 50(7): 24-29.
LAI J S, ZHAO W Y, ZHANG H Y, et al. Analysis of information security threats for quantum computing and countermeasures[J]. Information and Communications Technology and Policy, 2024, 50(7): 24-29.
[8] ISO/IEC. Information security — Digital signatures with appendix — Part 4: Stateful hash-based mechanism: ISO/IEC 14888-4: 2024[S]. 2024.
[9] 3GPP. Study on the support of 256-bit algorithms for 5G: TR 33.841, v16.1.0[S]. 2019.
[10] 3GPP. New WID on addition of 256-bit security algorithms: SP-231159[S]. 2023.
[11] 3GPP. New SID on study on enabling a cryptographic algorithm transition to 256-bits: SP-231788[S]. 2024.
[12] 3GPP. New WID on addition of milenage-256 algorithm: SP-231792[S]. 2024.
[13] 冯登国, 徐静, 兰晓. 5G移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813-1825.
FENG D G, XU J, LAN X. Study on 5G mobile communication network security[J]. Journal of Software, 2018, 29(6): 1813−1825.
[14] 唐明环, 彭浩楠, 王伟忠, 等. 5G 网络商用密码应用研究[J]. 信息安全研究, 2023, 9(4): 331-337.
TANG M H, PENG H N, WANG W Z, et al. Research on the application of commercial cryptography in 5G network[J]. Journal of Information Security Research, 2023, 9(4): 331-337.
[15] 3GPP. System architecture for the 5G System (5GS); Stage 2: TS 23.501, v18.5.0[S]. 2024.
[16] 中国通信标准化协会. 5G移动通信网 核心网网元功能技术要求: YD/T 3616-2019[S]. 2019.
CCSA. 5G teleommunication network general technical requirements of network function of core network: YD/T 3616-2019[S]. 2019.
[17] 3GPP. Technical specification group radio access network; NR; NR and NG-RAN overall description; Stage 2: TS 38.300, v18.3.0[S]. 2024.
[18] 梁敏, 罗宜元, 刘凤梅. 抗量子计算对称密码研究进展概述[J]. 密码学报, 2021, 8(6): 925-947.
LIANG M, LUO Y Y, LIU F M. A survey on quantum-secure symmetric cryptography[J]. Journal of Cryptologic Research, 2021, 8(6): 925-947.
[19] 董晓阳. 对称密码的量子分析法综述[J]. 密码学报, 2024, 11(1): 159-173.
DONG X Y. A Survey of quantum cryptanalysis of symmetric cryptography[J]. Journal of Cryptologic Research, 2021, 8(6): 925-947.
[20] 中国信息通信研究院. 后量子密码应用研究报告[EB]. 2023.
CAICT. Research report on the application of post quantum cryptography[EB]. 2023.
[21] NIST. Recommendation for key management, Part 1: General: SP 800-57 Part 1, Revision 4[S]. 2016.
[22] NIST. Transitioning the use of cryptographic algorithms and key lengths: SP 800-131A, Revision 2[S]. 2019.
[23] EKDAHL P, JOHANSSON T, MAXIMOV A, et al. A new SNOW stream cipher called SNOW-V[J]. Cryptology ePrint Archive, 2018.
[24] NIST. Secure hash standard (SHS): FIPS PUB 180-4[S]. 2015.
[25] NIST. SHA-3 Standard: permutation-based hash and extendable-output functions: FIPS PUB 202[S]. 2015.
[26] NIST. Module-Lattice-Based key-encapsulation mechanism standard: FIPS 203[S]. 2024.
[27] NIST. Module-Lattice-Based digital signature standard: FIPS 204[S]. 2024.
[28] NIST. Stateless hash-based digital signature standard: FIPS 205[S]. 2024.
[29] 中国密码学会. 关于全国密码算法设计竞赛算法评选结果的公示[EB]. 2020.
CACR. Publicity of the algorithm evaluation results of the national cryptographic algorithm design competition[EB]. 2020.
[30] 孙思维, 刘田雨, 关志, 等. 基于杂凑函数SM3的后量子数字签名[J]. 密码学报, 2023, 10(1): 46-60.
SUN S W, LIU T Y, GUAN Z, et al. SM3-based post-quantum digital signature schemes[J]. Journal of Cryptologic Research, 2023, 10(1): 46-60.
[31] 3GPP. Security architecture and procedures for 5G system: TS 33.501, v18.6.0[S]. 2024.
[32] 3GPP. 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 2: Algorithm specification:TS 35.206,v18.0.0[S]. 2024.
[33] 3GPP. Specification of the MILENAGE-256 algorithm set: An example set of 256-bit 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5, f5* and f5**; Document 1: General: TS 35.234,v0.1.0[S]. 2024.
[34] 3GPP. 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:TS 35.231,v18.0.0[S]. 2024.
[35] 3GPP. Network domain security (NDS); Authentication framework (AF): TS 33.310,v19.1.0[S]. 2024.
[36] IETF. Internet X.509 public key infrastructure certificate management protocol (CMP): RFC 4210[S]. 2005.
[37] IETF. Certificate management protocol (CMP) updates: RFC 9480[S]. 2023.
[38] IETF. Certificate management protocol (CMP) algorithms:

RFC 9481[S]. 2023.
[39] WANG C L, XUE W J, WANG J R. Integration of quantum-safe algorithms into X. 509v3 certificates[C]//Proceedings of 2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI). Piscataway: IEEE Press, 2023: 384-388.
[40] IETF. Composite signatures for use in internet PKI: draft-ounsworth-pq-composite-sigs-07[S]. 2022.
[41] IETF. Composite public and private keys for use in Internet PKI: draft-ounsworth-pq-composite-keys-04[S]. 2023.
[42] ISO/IEC. Information technology — open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks: ISO/IEC 9594-8: 2020[S]. 2020.
[43] 3GPP. Study on cryptographic algorithm transition to 256 bits: TR 33.700-41, v0.3.0[S]. 2024.43

[作者简介]

王聪丽（1994– ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为公钥密码基础设施、密码应用、商用密码应用安全性评估、5G 安全、量子安全等。

李金慧（1994– ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为密码应用安全、5G/6G 网络关键技术、网络安全、终端安全、量子安全等。

王靖然（1995– ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为网络安全、后量子密码等。

薛伟佳（1990– ），女，博士，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为密码应用、商用密码及密评、量子保密通信与密码融合应用等。

王锦华（1982– ），男，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为云计算、大数据安全、终端安全、密码应用、量子安全等。

王骞然（1994– ），女，中国电信股份有限公司研究院工程师、云网基础设施安全国家工程研究中心工程师，主要研究方向为 5G/6G 网络关键技术、密码应用安全、网络安全、量子安全等。