5G核心网商业密码部署方案研究

Research on Commercial Cryptography Deployment Scheme for 5G Core Network

贺晓博[1]，马田丰[2]，董留强[1]，尚　楠[1]（1. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007；2. 中国联合网络通信集团有限公司，北京 100033）

He Xiaobo[1], Ma Tianfeng[2], Dong Liuqiang[1], Shang Nan[1]（1. China Information Technology Designing & Consulting Institute Co., Ltd. Zhengzhou Branch, Zhengzhou 450007, China; 2. China United Network Communications Group Co., Ltd., Beijing 100033, China）

摘　要：

密码技术作为网络与信息安全保障的核心技术和基础支撑，在身份认证、信息加密、安全隔离、完整性保护和操作抗抵赖等方面发挥着不可替代的作用。当前商用密码的广泛应用还存在标准和生态等多方面的问题，需要推进标准制定、生态建设。研究并提出了5G核心网商业密码方案，该方案可用于提升5G核心网数据的安全性，为5G核心网提供更高的安全保障。

关键词：

5G核心网；商业密码；身份认证

doi：10.12045/j.issn.1007-3043.2026.08.011

文章编号：1007-3043（2026）08-0060-06

中图分类号：TN919

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

As the core technology and basic support for network and information security protection, cryptography plays an irreplaceable role in identity authentication, information encryption, security isolation, integrity protection, and operational non-repudiation. Currently, the widespread application of commercial cryptography still faces many obstacles in standards and ecology, requiring the promotion of standard and ecological construction. The commercial cryptography deployment scheme suitable for the 5G core network is studied and proposed, which can enhance the security of the 5G core network and provide higher security guarantees for it.

Keywords：

5G core network; Commercial cryptography; Identity authentication

引用格式：贺晓博，马田丰，董留强，等. 5G核心网商业密码部署方案研究[J]. 邮电设计技术，2026(8)：60-65.

1 概述

随着5G技术的迅速普及[1]，网络的复杂性和多样性也随之增加，导致传统的安全防护措施面临诸多挑战。5G核心网引入了虚拟化、网络切片等新技术，同时网元间的服务化接口采用http协议，改变了传统网络的安全边界，进而引发了一系列新的安全风险[2-3]。且随着5G核心网在工业互联网、智能城市等垂直行业中的广泛应用，网络安全的重要性愈发突出。5G网络不仅需要满足高可用性和低延迟的要求，还要确保信息的机密性和完整性[4]。

密码技术作为网络与信息安全保障的核心技术和基础支撑，在身份认证、信息加密、安全隔离、完整性保护和操作抗抵赖等方面发挥着不可替代的作用[5]。而量子计算对传统密码算法的威胁以及未来可能出现的新型攻击手段也是5G面临的新挑战。

国密算法在维护国家数据主权方面发挥着至关重要的作用，是国家安全战略中不可或缺的一部分。通信网络是国家关键的基础设施，在通信网中推广落地国密算法具有重要意义。随着技术的不断进步和应用需求的增加，国密算法将继续发展，为构建安全可靠的信息社会提供有力支撑。

收稿日期：2026-06-01

本文立足数据主权的安全防护，聚焦从终端到5G核心网的主认证及管理面过程改造，推进商用密码技术的落地应用。

2 环境及挑战

5G网络对数据传输速度和容量的要求较高，因此加密算法既需要符合安全性要求，又要具备高效性。如何根据5G网络的特性，选择和设计适合、安全的密码算法，使其同时具备安全性和高效性是当前亟待解决的重要问题。

在5G核心网中，国产密码算法也得到了广泛的应用。目前，我国主要使用的国产密码算法有SM2、SM3、SM4和祖冲之算法（ZUC）。

a）SM2是一种非对称加密算法，可以用于数字签名、密钥协商和加密通信等方面。

b）SM3是一种哈希算法，可以用于数据完整性校验和数字签名等方面。

c）SM4是一种对称加密算法，可以用于数据加密和解密等方面。

d）祖冲之算法是一种由中国自主研发的流密码算法，是移动通信3GPP机密性算法EEA3和完整性算法EIA3的核心。

在5G全球标准制定中，加密技术是一种全球可用的通用技术，但各国在算法选择、标准制定和应用实践等方面的权力存在竞争与冲突。例如在使用ECC和RSA的公钥密码算法中，各国都在尽力推广并保护自身的算法技术，并在全球范围内影响或限制其他算法的应用，避免他国算法普及带来的后门漏洞、监听风险等安全威胁。因此，在使用国产密码时，互联互通也是一个亟待解决的重要问题。

3 软硬件生态

随着《密码法》及《关键信息基础设施安全保护条例》的实施和密码测评的推进，商用密码技术和产品正在快速发展，逐步为基础电信网络和信息系统服务构筑商密能力[6-7]，但也存在较多挑战。当前5G核心网商密应用面临的主要挑战和问题如下。

a）商密算法未被完全纳入国际标准。大量协议标准未对商密应用进行定义，存在互联互通风险；终端和大网存在互操作性兼容性风险，国标与国际主流安全协议标准无法互通，当前标准进展较慢。

b）商密软硬件生态待完善。

（a）硬件生态。商密算法缺少硬件生态，性能差距较大。出于安全考虑，商密的算法设计本身复杂度相对较高，在同等硬件基础上，软件实现的商密算法性能较低；硬件生态缺乏对商密算法的支持，部分计算设备目前仍以X86架构处理器为主，而Intel处理器AVX指令集支持AES算法加速，不支持商密加速。在上述2个因素的影响下，在业务处理场景中，商密算法性能差距较大。

（b）软件生态。大部分开源组件不支持商密，主流开源软件基于IETF国际标准实现，不支持商密算法。

c）缺少CT密评方案指导。国标GB/T 39786-2021缺少在CT领域的应用实践；传统外挂式方案缺少标准定义，影响CT系统架构，新增业务断裂点。

商用密码的广泛应用还存在标准和生态诸多障碍，需要推进标准制定、生态建设，并研究适用于基础通信网络的商密应用及密评方案，解决商密应用和推广的根本问题。

4 商密在5G核心网中的应用分析

商用密码，即ZUC算法（也称为祖冲之算法）是根据128 bit的初始密钥和128 bit的初始向量，输出32 bit的密钥序列，用以对数据进行机密性和完整性保护，其在业务面及管理面应用时的场景及挑战如下。

4.1 业务面

4.1.1 支持情况

当前核心网标准接口协议中，只有N1口支持国密算法，其他接口均不支持国密，具体如表1所示。

从表1可以看出，在业务面，目前3GPP国际标准中协议和算法整体缺少对国密算法的支撑，仅N1口和空口支持ZUC算法，其他接口均涉及互联互通问题，故须优先推动商密纳入3GPP、IETF等产业标准。

在设备层面，目前厂家AMF设备均支持ZUC加密算法，ZUC算法保护AMF与UE之间的NAS层和AS层信令的机密性和完整性。启用ZUC算法需要UE和AMF的同步支持，故启用ZUC算法的前提是完成周边的商密应用改造。

4.1.2 UE认证应用分析

目前5G网络中主要有5G-AKA认证和EAP-AKA'认证，密码算法主要在生成认证向量时使用。在5G-AKA流程中，UDM、UE均使用基于HMAC-SHA256算法的KDF函数计算预期响应，AUSF使用

表1　商密改造对核心网标准接口协议的影响

内容	涉及网元	3GPP等国际标准现状	商密改造影响
用户身份加密（SUPI）	USIM、终端、UDM	3GPP引用SECG标准Profile A和Profile B 2套参数，未包含国密	UDM不能解密UE发送的密文，导致UE注册失败
用户认证	USIM、终端、AMF、AUSF、UDM	5G-AKA/EAP-AKA’、AES-128、KDF、HMAC-SHA-256，未采用国密算法	UDM生成认证向量，现有终端不能校验，导致认证失败；AMF，AUSF，ME：不支持商密认证，导致认证失败
N1	终端、AMF、gNB	SNOW 3G、AES-128、ZUC-128	已满足
N2	gNB、AMF	DTLS、IPSec IKEv2安全通道，未采用国密算法	所有NAS信令和RAN管理均失败
N3/N4/N6/N9	gNB、SMF、UPF	IPSec IKEv2安全通道、AES-128，加密；AES-128-CBC，完整性保护；AES-XCBC-MAC-96、未采用国密算法	对接失败，数据面相关功能失效
N32	SEPP	N32-c TLS1.2/1.3、N32-f、TLS/PRINS，未采用国密算法	对接失败，影响所有漫游业务
SBI	UDM/NRF等所有NF	TLS、OAuth，未采用国密算法	对接失败，影响所有漫游业务和所有非漫游NF之间交互

SHA256算法计算预期响应的哈希值。此外，5G-AKA和EAP- AKA’2种认证机制均采用MILENAGE算法，由UE、UDM/ARPF等网元协同实现，其核心算法E_K采用128 bits的AES算法（见图1）。

若对该认证过程进行国密算法替换，可使用SM3算法替换SHA256算法，使用SM4算法替换AES算法，对5GC的UE、UDM/ARPF、AUSF网元配置经国家密码管理部门认可的SM3/SM4密码算法模块，并设置优先

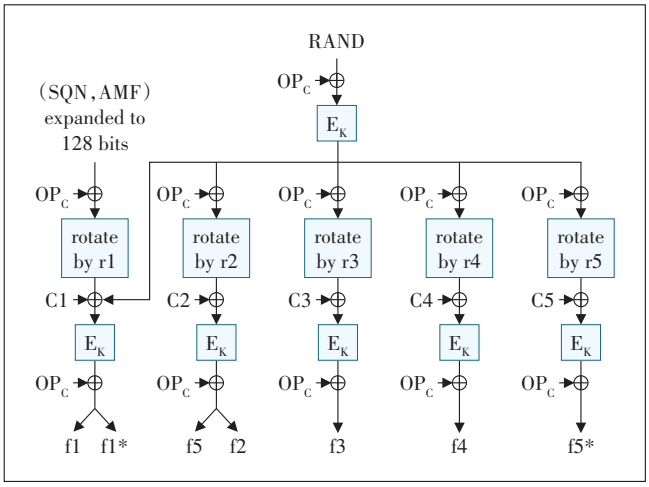

图1　UE认证应用核心算法

启用SM3/SM4算法，即当通信双方都配置SM3/SM4时，会优先启用该算法。但目前5G接入认证环节不支持算法配置选择机制，若实施国密改造，还需增加密码算法协商协议以及关键字段定义，改动难度较大，可使用多算法协商AKA方案。

在UE的USIM卡和UDM/ARPF升级支持多个密码算法套件后，多算法协商方案流程如图2所示。

a）UE发送初始化注册请求（Initial Registration Request）给网络侧，包括USIM卡的标识符信息SUCI（其中包含了标识符信息SUPI），SUCI通过相关网元被转发到归属网络UDM。

b）UDM对每个Nudm_Authenticate_Get Request消息创建一个5G HE AV（RAND，AUTN，XRES，CK，IK）。UDM可根据算法选择策略选择应使用的密码算法套件AKA_AS。

（a）未升级的UDM应按照原协议执行，已升级的UDM可根据算法选择策略选择应使用的密码算法套件AKA_AS。首先，UDM根据SUCI查询对应的USIM的签约数据，包括USIM的密码算法套件支持列表（USIM_AS_LIST）。然后，UDM获取网络侧本地定义的密码算法套件列表（AKA_AS_LIST）。再后，UDM查看标记为优先的密码算法套件（比如密码算法套件2-SM3/SM4）是否在USIM_AS_LIST中，如果在，则将AKA_AS设置为优先的密码算法套件；如果不在，则将AKA_AS设置为USIM_AS_LIST和AKA_AS_LIST共有的且可用的密码算法套件（比如密码算法套件1-AES）。如果USIM_AS_LIST不存在，则将AKA_AS设置为密码算法套件1。

（b）UDM将AKA_AS（一般是索引值）保存在AV中AMF（Authentication Management Field）的预留位中。AMF的第1~7和第8~15位是预留位，默认是0，可以选择其中固定的位置保存AKA_AS。

（c）UDM根据AKA_AS对应的密码算法套件为f1、f2、f3、f4、f5、f1*、f5*函数的底层密码算法，计算5G HE AV（RAND，AUTN，XRES，CK，IK）。

c）UDM在Nudm_UEAuthentication_Get Response消息中向AUSF返回所请求的5G HE AV，并指示5G HE AV用于5G AKA。若Nudm_UEAuthentication_Get请求中包含SUCI，UDM将在Nudm_UEAuthentication_Get响应中包含SUPI。

d）AUSF应临时保存XRES*及接收到的SUCI或SUPI。AUSF可保存KAUSF。

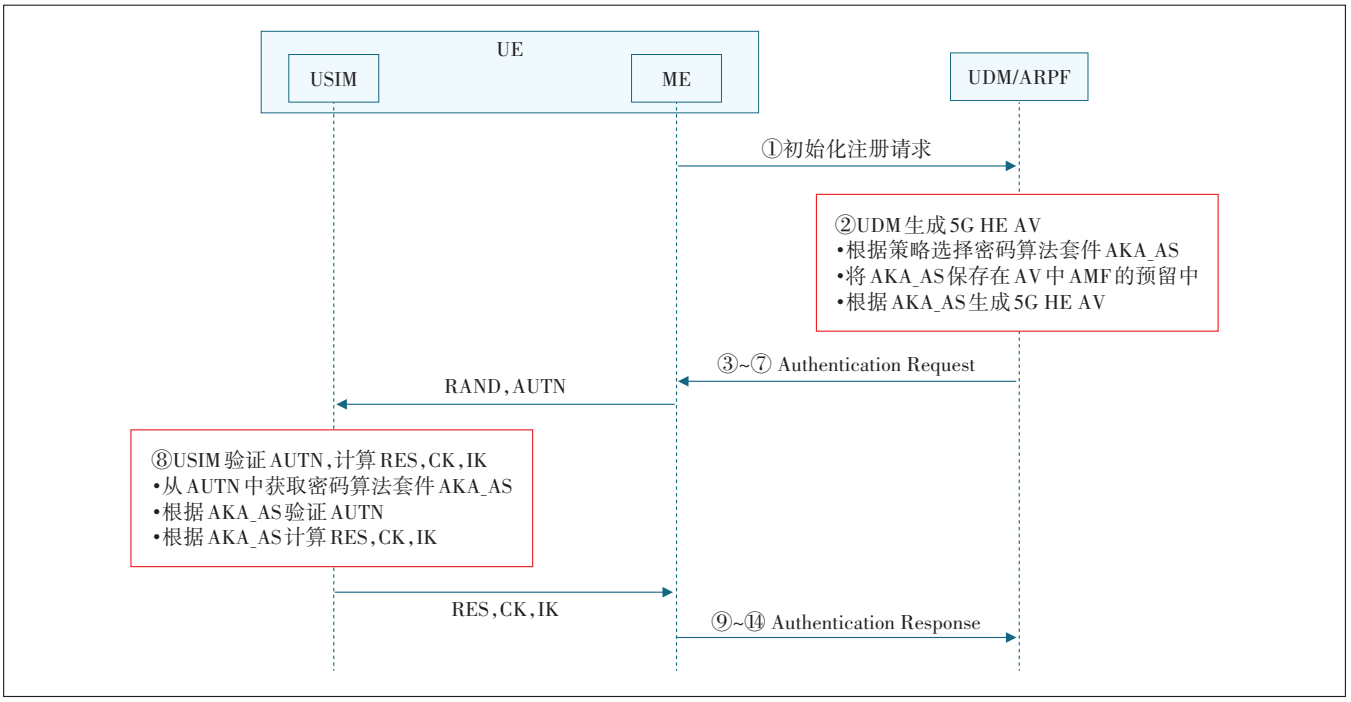

图2　多算法协商方案流程

e）AUSF应基于从UDM/ARPF接收到的5G HE AV生成一个5G AV。从XRES*计算出HXRES*，从KAUSF推衍出KSEAF，然后用HXRES*和KSEAF分别替换5G HE AV中XRES*和KAUSF。

f）AUSF应移除KSEAF，通过Nausf_UEAuthentication_Authenticate响应将5G SE AV（RAND，AUTN，HXRES*）发送至SEAF。

g）SEAF应通过NAS消息（Auth-Req）向UE发送RAND和AUTN。该消息还应包含被UE和AMF用于标识KAMF和部分原生安全上下文的ngKSI，以及ABBA参数。ME应向USIM转发NAS消息（Auth-Req）中的RAND和AUTN。

h）USIM收到RAND和AUTN后，USIM应检查AUTN是否被接受，以此来验证认证向量是否为最新向量。若验证通过，USIM应计算响应RES，并向ME返回RES、CK、IK。若USIM使用3GPP TS 33.102中描述的转换函数c3，从CK和IK计算出Kc（即GPRS Kc）并将其发送给ME，ME应忽略该GPRS Kc，且GPRS Kc不应存储在USIM或ME上。USIM从AUTN的AMF中获取AKA_AS，并根据AKA_AS指定的密码算法套件验证AUTN以及计算RES、CK、IK和Kc。

i）ME应从RES计算RES*，从CK‖IK推衍出KAUSF，从KAUSF推衍出KSEAF。接入5G的ME应在认证期间检查AUTN的AMF字段的“separation bit”是否设为1。“separation bit”是AUTN的AMF字段的第0位（“separation bit”不能再用于运营商特定目的）。

j）UE应在NAS消息认证响应中将RES*返回给SEAF。

k）SEAF应从RES*计算HRES*，并比较HRES*和HXRES*。若两值一致，SEAF应从服务网的角度认为认证成功。若不一致，SEAF应认为认证失败，并向AUSF指示失败。

l）SEAF应将来自UE的相应SUCI或SUPI通过Nausf_UEAuthentication_Authenticate Request消息发送给AUSF。

m）当接收到包含RES*的Nausf_UEAuthentication_Authenticate Request消息时，AUSF可验证AV是否已到期。若AV已过期，AUSF可从归属网络的角度认为认证不成功。AUSF应将接收到的RES*与存储的XRES*进行比较，若RES*和XRES*一致，AUSF应从归属网络的角度认为认证成功。

n）AUSF应通过Nausf_UEAuthentication_Authenticate Response向SEAF指示认证是否成功。若认证成功，则应通过Nausf_UEAuthentication_Authenticate Response将KSEAF发送至SEAF。若AUSF在启动认证时从SEAF接收到SUCI且认证成功，AUSF还应在

Nausf_UEAuthentication_ Authenticate Response中包含SUPI。

若认证成功，SEAF应把从Nausf_UEAuthentication_Authenticate Response消息中接收的密钥KSEAF作为锚密钥。然后SEAF应从KSEAF、ABBA参数和SUPI推衍出KAMF，并向AMF提供ngKSI和KAMF。

如果SUCI用于此认证，SEAF应仅在接收到包含SUPI的Nausf_UEAuthentication_Authenticate Response消息后才向AMF提供ngKSI和KAMF；在服务网获知SUPI之前，不会向UE提供通信服务。

4.2 管理面

4.2.1 部署情况

如表2所示，当前核心网管理面逻辑框架整体上包括人机接口、北向接口、南向接口以及自身重要数据存储这几个部分。

表2　核心网网管密码业务场景

类别	密码业务场景	协议算法	实现方案	影响与风险
人机接口	浏览器访问MAE的Portal	HTTPS	MAE（OMC等）：支持跟国密浏览器对接，支持国密安全传输，支持国密双证书管理，支持对其他浏览器兼容	-
北向接口	对接堡垒机等认证系统	REST、LADP、Radius等	MAE（OMC等）：支持国密安全传输和国密双证书管理，北向对接系统同步支持国密	目前LDAP、Radius缺少国密标准
	与上层OSS对接，涉及告警、性能、配置等多个北向接口	REST/MML/Socket/SFTP/Syslog	MAE（OMC等）：支持国密安全传输和国密双证书管理、国密模式开关控制，同时兼容非国密的OSS对接方式 OSS：同步支持国密	a）标准：SSH、SFTP无标准 b）开源：OpenSSH等开源软件改造 c）性能：大量OSS需要同步支持国密，改造周期长，容易引入性能风险
南向接口	与VNF、eSight、FS等通信	MML/SOAP/REST/SFTP/FTPS/Netconf/SNMPv3/Syslog/NTP/GRPC/SSH	MAE（OMC等）：支持国密安全传输和国密双证书管理、国密模式开关控制，同时兼容非国密的网元/VIM/PIM对接方式 网元：同步支持国密	a）标准：针对SNMP，暂无国密标准协议 b）开源：针对SNMP，涉及国际标准刷新及开源软件改造 c）性能：涉及大量南向设备同步支持国密，且容易引入性能风险
重要数保护	重要数据加密存储	SM4/SM3	MAE（OMC等）：支持国密密钥管理及加解密算法，支持非国密到国密的切换和回退，支持工作密钥生命周期管理	国密模式切换时，可能涉及大量数据的重新加解密，涉及业务中断

4.2.1.1 北向商密应用影响分析

北向商密应用涉及大量北向系统（10+）的配合改造，改造和调测周期长，且北向改造需要考虑北向系统双向改造，同时考虑性能数据。

由于国密算法的性能比传统算法低，改造后北向数据上报存在很大的性能风险，可能会导致PM/FM/Log上报延迟或数据缺失，批量MML下发延迟或失败，须通过管理面扩大资源解决。

4.2.1.2 南向商密应用影响分析

南向商密应用涉及大量南向设备（如xx大区有1 000+的网元）的配合升级和改造及调测，周期长。

由于国密算法的性能比传统算法低，改造后管理面采集南向数据时会存在很大的性能风险，可能会导致PM/FM/Log上报延迟或数据缺失，批量MML下发延迟或失败，需通过管理面扩大资源解决。

由于南向对接属于内部系统对接，3GPP没有定义其加解密实现，而是由厂家实现。目前，运营商和工信部暂不建议对南向的商密改造，只能通过防火墙防护等方式保证南向网络数据传输的安全性。

4.2.1.3 移动通信网网管商密方案建议

综上，在管理面建议优先考虑人机接口、重要数据保护，南向接口明确不做要求，北向接口视运营商改造情况来实施。

4.2.2 应用分析

核心网网管OMC改造聚焦人机接口及系统重要数据存储。核心网网管纳管大量的业务网元，在商密改造过程中，需要确保5G网络的高可靠，避免影响网络的整体运行。移动通信网网管商密方案拓扑如图3所示。

4.2.2.1 人机接口安全访问

a）部署商密安全浏览器与VPN安全网关。在国密安全浏览器与VPN安全网关之间建立传输层SSL安全传输通道，对用户与OMC系统之间传输的所有通信数据进行加密和完整性保护。

b）网管配套支持商密浏览器。商密浏览器应能够适配OMC。

4.2.2.2 重要数据安全存储

a）主备容灾。大区主备OMC同时对接主用、备用密码平台，实时检测主备用密码平台状态，选择可用的密码平台。

b）国密算法。OMC加解密框架支持商密SM3、SM4算法。

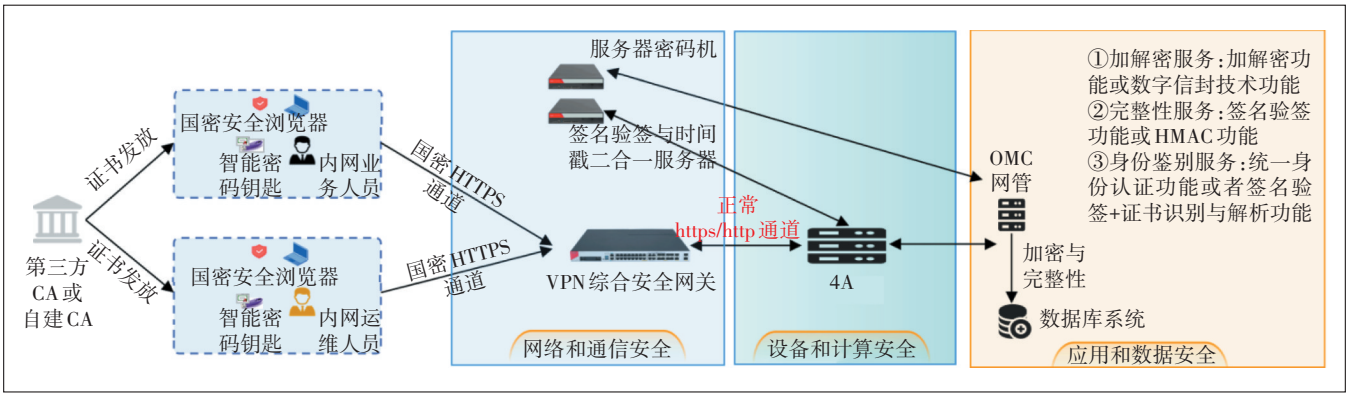

图3　移动通信网网管商密方案拓扑

c）密钥管理。密码服务平台用于提供统一的密码服务能力。

d）不可逆算法。OMC对接加密机获取HMAC_SM3密钥，利用该密钥及HMAC_SM3算法来加密口令及重要数据。

e）可逆算法。OMC对接加密机获取SM4密钥，利用该密钥及SM4算法来加密口令及重要数据。

f）惯性运行。加密机故障不能影响OMC的运行，OMC缓存机制实现惯性运行。

5　结论建议

综上，基于现有标准和现有生态环境，5G核心网的商用密码可从以下2个方面进行部署。

a）认证改造。在终端到核心网的认证过程中引入商用密码，增强终端与核心网之间的认证安全性。此过程主要涉及到UDM设备，需要进行相应的版本升级。

b）管理面改造。在现有OMC系统中引入商用密码，部署商密安全浏览器和VPN安全网关，提升网络管理的高可靠性和可用性。

商用密码的应用也是5G网络安全的重要组成部分。尽管5G标准中引入了多种密码技术，但在实际应用中，现有的5G安全标准主要采用国际通用的密码算法，而我国的商用密码仅在特定场景下得到应用，这使得5G网络的安全防护能力相对不足，亟需加强商用密码技术的应用。同时，为了增强网络的安全防护能力及国家数据主权的保护力度，也需要推进商用密码技术的广泛应用。在核心网中，可以集成多种商用密码算法，确保数据在传输和存储过程中的机密性与完整性。随着5G网络的普及和网络空间攻防对抗形势的加剧，作为关键信息基础设施的5G移动通信网的安全保护愈发紧迫。因此，推进商用密码技术在5G网络中的应用，不仅可以提升网络的安全防护能力，还能满足政府、企业等行业的高安全需求。

参考文献：

[1] 张阳. 记者手记：商用五周年，数说5G高质量发展[EB/OL]. [2026-03-06]. https://tech.huanqiu.com/article/4I6K34AfasW.

[2] 曹刚，关先锋. 利用网络微分段技术增强5G电信云安全性的研究[J]. 邮电设计技术，2025(5)：62-68.

[3] Sysdig. Twenty 23：global cloud threat report[EB/OL]. [2026-03-18]. https://sysdig. com/content/c/pf-2023-global-cloud-threatreport? x=u_wfri.

[4] 江小平. 基于智慧家庭应用的组网方案[J]. 物联网技术，2021，11(1)：39-41.

[5] 王瀚洲，周洺宇，刘建伟，等. 5G网络安全威胁发现及解决方法综述[J]. 信息安全研究，2024，10(4)：340-346.

[6] 国家法律法规数据库. 中华人民共和国密码法[EB/OL]. [2026-03-18]. https://flk.npc.gov.cn/detail?id=ff8080816f3cbb3c016f5acf6a244210&title= % E4%B8%AD% E5%8D% 8E% E4%BA% BA% E6%B0%91%E5%85%B1%E5%92%8C% E5%9B% BD% E5%AF%86%E7%A0%81%E6%B3%95.

[7] 中央网络安全和信息化委员办公室. 关键信息基础设施安全保护条例[EB/OL]. [2026-03-18]. https://www.cac.gov.cn/2021-08/17/c_1630785976988160.htm.

作者简介：
贺晓博，毕业于北京邮电大学，高级工程师，学士，长期从事云核心网网络及安全相关的研究、规划、咨询及设计工作；马田丰，毕业于北京大学，工程师，硕士，主要从事移动核心网网络安全相关研究和建设工作；董留强，毕业于华中科技大学，高级工程师，学士，主要从事移动核心网、通信云、创新业务平台等专业的研究和设计工作；尚楠，毕业于重庆邮电大学，高级工程师，硕士，主要从事移动核心网、通信云、创新业务平台等专业的研究和设计工作。