视点聚焦

5G 安全技术与标准

杨志强，粟栗，齐旻鹏，杨波
（中国移动通信有限公司研究院，北京 100053）

摘　要：移动通信从 4G 演进到 5G 的过程中，在网络演进和业务需求的促进下，安全设计的理念进一步完善，安全能力更加丰富。指出 5G 网络安全的设计理念是在开放的环境下构建安全的网络与服务，基于对 3GPP、ITU、GSM 中的 5G 安全标准的综合分析，梳理出网络自身安全保障、垂直行业支撑、安全测评认证 3 条主线。基于这 3 条主线，对 5G 网络中引入的安全新技术、安全新能力、安全新风险进行深入分析，并对 5G 安全未来发展趋势和重点工作提出建议。

关键词：5G 安全；安全规范；网络安全；安全能力；安全测评；发展趋势
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020317

Overview and prospect of 5G security

YANG Zhiqiang, SU Li, QI Minpeng, YANG Bo
China Mobile Research Institute, Beijing 100053, China

Abstract: From 4G to 5G, as the result of network evolution and service promotion, the concepts and principles of security in design were deeply integrated, the security capabilities were enhanced. The root of 5G security design-building secure networks and services in the open environment were analyzed. Furthermore, according to the understanding of the 5G security specifications designed by 3GPP, ITU and GSMA, the security framework and these new technologies were analyzed in detail from three aspects: network security assurance, service security capabilities and security assessment methodologies. The overview of 5G security trends and the key works in the long run were summarized.

Key words: 5G security, security specification, network security, security capability, security assessment, development trend

1　引言

移动通信从 20 世纪 80 年代发展至今，已经近 40 年。在大约 10 年一代的发展过程中，移动通信技术不断超越自己，形成质的飞跃。2015 年，ITU（International Telecommunication Union）定义了 5G 的 eMBB（enhanced mobile broadband）、mMTC（massive machine type communication）、

收稿日期：2020−08−19；修回日期：2020−12−09
通信作者：粟栗，suli139@139.com

uRLLC（ultra-reliable and low latency communication）三大业务场景[1]，提出了包括峰值速率、移动性、时延、体验速率、连接数密度的新指标。2020 年 7 月 3 日，第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）正式发布 5G R16 版本规范，同时也成为 ITU 官方唯一认可的 5G 标准，标志着 5G 技术走向成熟。

5G 移动通信技术是通信历史上的又一次重大革新，将移动通信的领域从“人与人通信”扩展到“物与物连接”。同时，5G 的作用已不仅限于信息处理和传递，更成为承载万物智慧连接、激发科技创新活力、升级产业竞争实力、促进经济发展质量的新引擎[2]。一方面，5G 作为新一代通信的基础设施，自身安全性不言而喻；另一方面，随着 5G 建设与商用的全面铺开，5G 网络与垂直行业应用深度融合放大了 5G 的安全影响范围，需要有更高的安全保障。正是因为 5G 成为整个社会、整个国家的基础设施，其安全问题受到了全球高度关注。目前，多个国家已经发布 5G 安全战略[3]，将 5G 网络的安全性与国家安全、经济安全和其他国家利益以及全球稳定性相关联。

在移动通信网络中，安全与网络及业务伴生发展。从网络演进的角度看，5G 更加开放、网络架构更加灵活，需要更好的安全手段保护自身安全；从业务支持的角度看，5G 更加灵活与定制化，需要更丰富的安全机制支持。正是在上述因素的驱动下，5G 安全体系的构建以更开放、更灵活的网络环境为前提，以实现网络自身安全防护、为业务提供安全服务为目标，在 4G 安全体系的基础上演进形成。在全球学者、专家的努力下，以 3GPP 安全与隐私工作组（SA3）为主的多个国际标准化组织共同合作，形成了 5G 安全系列标准。这些标准中定义了 5G 网络机密性、完整性、用户隐私保护等安全机制的增强，并为切片和移动边缘计算等新的网络服务模式、5G 垂直行业典型场景提供了安全支撑，实现了 5G 系统较为全面的安全保障体系。

本文从需求与演进的思路分析 5G 安全体系的演进与形成过程，然后以 3GPP、ITU、GSMA 制订的 TS33.501[4]等重要 5G 安全标准为参考，全面介绍 5G 网络中的安全关键新技术，并展望 5G 安全未来发展方向。

2 5G 网络安全演进需求

移动通信系统最大的特点就是“移动性”，即用户在大范围内移动时，可以不间断地享受电话、消息、数据等通信业务。因此，从 2G 开始就支持漫游功能，用户仅在一个运营商注册，就可以享受由不同运营商提供的网络服务，实现了全球移动通信。

为了提供可移动的通信能力，移动通信系统设计了“终端–接入网–核心网–互联互通”的基础架构，这个逻辑架构从 2G 到 5G 网络都得以保持和完善。同时，在移动通信网络代际演进的过程中，在业务需求、网络与 IT 技术的不断驱动下，每代网络都进行了大量技术革新。基于业务需求与 IT 技术的演进，与 4G 相比，5G 网络采用了虚拟化、服务化的核心网架构，并支持移动边缘计算、切片等新型网络服务模式。归纳 5G 网络的逻辑架构及其主要新特性如图 1 所示。

2.1 开放网络环境促进 5G 安全防护体系完善

随着移动通信技术的普及，移动互联网业务大量发展、网络自身 IT 和 CT 的日渐融合，移动通信网络在组网、设备、业务等多个方面逐渐开放。开放的网络意味着暴露面增加，进而导致对象之间的信任程度降低。不同代际移动通信网的信任机制的差别见表 1，在 2G 设计时，网络封闭、业务封闭，运营商之间的网络互信，仅认为终端不可信；3G 设计时，网络与业务部分开放，不再认为网络对终端完全可信；4G 设计时，网络已经较为开放，网络租赁业务发展，因此也不再认定运营商之间的互通可信等。演进到 5G，随着多样

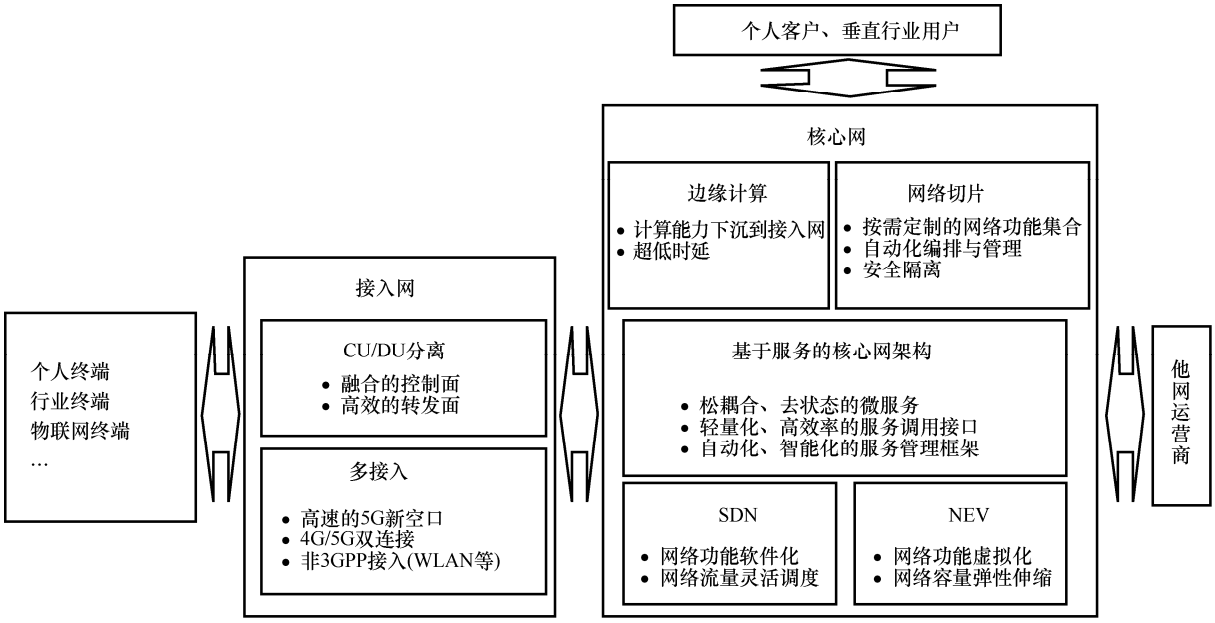

图 1　5G 网络逻辑架构及其主要新特性

表 1　移动通信网信任机制演进

	实体可信				链路安全		
	终端对网络	网络对终端	运营商与业务服务商之间	运营商之间	空口数据传输	运营商内部数据传输	运营商之间数据传输
1G	信任	信任	—	—	—	—	—
2G	信任	非信任	信任	信任	非信任	信任	信任
3G	非信任	非信任	部分信任	信任	非信任	部分信任	非信任
4G	非信任	非信任	非信任	部分信任	非信任	部分信任	非信任
5G	非信任	非信任	非信任	部分信任	非信任	非信任	非信任

终端接入能力的支持、SBA（service based architecture）[5]、网络设备虚拟化等技术的引入，网络越来越开放、网元之间的互通路径越来越多；因此，必须设计一个更安全的体系，保障终端、漫游网络、归属网络、业务系统等实体的安全需求。

正是因为面临更开放的环境，也引入了更多的安全风险；与 4G 相比，在 5G 网络的设计中引入了大量的安全新方案。

（1）不再与存在较多风险的 2G 网络进行互操作。

（2）增强用户接入认证机制：考虑归属网络和漫游网络不完全可信而产生的内部攻击风险，在 5G-AKA 算法中，增加了归属网络对漫游网络的认证，解决了可能存在的漫游运营商欺骗归属运营商的风险。

（3）增强的数据安全：5G 网络沿用了 4G 的密码算法，对机密性和完整性进行保护，同时还增加了对用户面数据的完整性保护，避免了从空口对用户面数据进行篡改的攻击[6]。

（4）增强的用户隐私保护：在 2G 到 4G 网络中，虽然使用临时移动用户标识（temporary mobile subscriber identity，TMSI）保护国际移动用户标识（international mobile subscriber identity，IMSI），但 IMSI 仍然需要在开机等环节明文在空口传输，

存在一定的用户隐私泄露风险；在 5G 网络中，使用了数字证书和公钥算法对用户永久标识符（subscriber permanent identifier，SUPI）进行保护，形成用户隐藏标识（subscription concealed identifier，SUCI），且每次使用时加密的 SUCI 都不同，避免了对用户的识别与跟踪等风险。

（5）引入服务域安全：由于 SBA[7-8]替代了传统的专用接口，在内部网元互访变得更开放、便捷，暴露面也同时增大；基于核心网网元之间的互通不完全可信的考虑，引入设备间认证的安全机制，保障互访设备的真实性。

（6）强调的虚拟化安全：5G 网络中对云和虚拟化安全进行了要求，避免了虚拟化引入产生的两个方面的新风险；一是虚拟化的系统、设备自身存在安全风险；二是虚拟化的解耦能力，使原本一体的设备接口暴露，增加了新的暴露面，需要安全机制保障。

（7）增强了运营商互通安全保护：5G 网络中不再认为运营商之间互通是可信的，基于该前提，在运营商之间增加了 SEPP（security edge protection proxy，安全边界保护网关）网元[4]，对信令进行安全保护；避免了 SS7、Diameter 等协议被篡改的风险。

2.2 丰富的业务场景促进 5G 网络安全能力服务化

与 4G 相比，5G 网络拥有更开放的新架构与更为丰富的网络能力，可以向垂直行业提供更丰富、更完善的安全服务。

（1）5G 三大应用场景的设计与垂直行业的加入，大量新型终端的接入对网络接入认证提出新需求，促进 5G 网络定义基于 EAP 的方式支持更多类型的认证，以适配多样的接入终端。

（2）网络切片的能力将“专线”的概念延伸到“专网”，促进安全能力服务化、定制化：一方面，切片提供了定制化的安全隔离、认证等能力，实现了安全能力服务化；另一方面，虚拟化、软件化的技术与实施作为切片实现基础，也提出了新的安全防护需求。

（3）移动边缘计算为客户提供了区域化、现场化的业务解决方案，同时也对 UPF 等电信级网元设施提出了下沉后的安全保护新需求。

（4）为了更好地满足 5G 行业客户的需求，5G 还将安全作为一种服务为客户提供：一是进一步将基于 3GPP 凭证的应用层认证和密钥管理项目（authentication and key management for applications based on 3GPP credential，AKMA）[9]向客户开放；二是基于网络能力开放接口，可以将扫描、监控等安全能力作为服务提供给客户。

综上所述，在 5G 网络中新增或增强的安全手段一方面满足了 5G 自身安全防护与保障的需求，另一方面可以为新业务场景提供服务。虽然 5G 中安全手段的设计理念是在开放网络环境下提供更好的安全防护能力，但同时也需要认识到安全不是绝对的，所以在安全机制的设计过程中仍然需要考虑现实环境，包括计算能力、网络运行的环境、终端的形态、安全攻防水平、管理机制等因素。同时，安全也是有成本和代价的，网络运营者通常需要综合评估安全机制实施带来的用户体验或业务连续性的影响和实施成本。

3 5G 安全标准体系

移动通信网络的技术标准是网络的设计文档和统一的实现要求。在 3GPP、ITU、GSMA、ISO 等标准组织的共同努力下，5G 安全系列标准在前几代通信系统安全标准的基础上演进形成。3GPP 在 2020 年 7 月发布的 R16 系列规范是 5G 的第一个演进版本，也是 ITU 唯一认可的 5G 技术标准，标志着 5G 技术从形成到成熟。其中，服务与系统架构（service and system architecture，SA）下的第三工作组（SA3）发布了包括技术标准（technical specification，TS）和技术报告（technical report，TR）在内的 29 个文档，形成了 5G 的系列安全要求。

从国际技术标准发展的角度看，5G 网络安全标准体系在 4G 的基础上进一步演进形成；归纳来说，逐渐以网络自身安全保障、业务需求的安全能力、网络与业务安全测评为 3 条主线，如图 2 所示。

第一条主线是 5G 系统本身的安全机制增强。即安全技术在 5G 系统的应用，实现更安全的 5G 端到端系统。一方面，5G 网络自身的演进带来了一些新的安全需求，在设计过程中加以考虑并形成了标准；另一方面，产业界和学术界发现的前几代系统的安全风险和设计缺陷也在新的代际系统中进行了修补和改进，从而形成了相关的标准。这条主线中的技术标准主要是由 3GPP 制订的，在基础协议等领域引用到 IETF、W3C 等标准组织设计的技术标准。总的来说，与 4G 相比，5G 的安全体系设计更加完善、安全机制更加全面。

第二条主线是 5G 的新业务场景驱动而形成的安全新能力。由于越来越多的垂直行业加入，新行业应用增加了 5G 安全的复杂度，也对 5G 安全提出了新的诉求。因此，各个标准组织在制订 5G 安全标准时，均考虑了应用场景和垂直行业的安全诉求。例如，3GPP 在 R15 主要针对 eMBB 场景进行了安全设计，在 R16 时引入了 uRLLC 和 CIoT 的安全机制研究和设计。此外，垂直行业的需求促进了切片、边缘计算、能力开放等新技术的发展，也提出了安全的新需求，促进了安全新能力的完善。

第三条主线是对设备的安全认证和评估标准。安全认证和评估标准用来帮助电信运营商及监管机构评估和度量网络设备的安全性。这套标准在 4G 时代就已经起步，由 GSMA 和 3GPP 协作推动，在 5G 时代，这套标准逐渐完善与形成。由 GSMA 编制的网络设备安全保障体系（network equipment security assurance scheme，NESAS）是一套指引性文档[10]，制订了设备安全审计评估的方法论、流程等，其中引用了 3GPP 制订的 SCAS（security assurance specification）系列规范作为测试评估的技术要求。

4　5G 网络安全防护体系演进

4G 自身的安全体系在理论上已经较为完善，演进到 5G 后，在网络与业务发展、攻防技术提升的驱动下，安全机制更完善、安全能力更丰富。根据 TS33.501[11]标准可知：5G 网络继承和增强了 4G 的安全架构，与 4G 网络的安全功能对比，除了新增的 SBA 安全能力外，在接入网域的安全机制变化明显，在用户域、网络域和应用域的安全机制平滑演进。

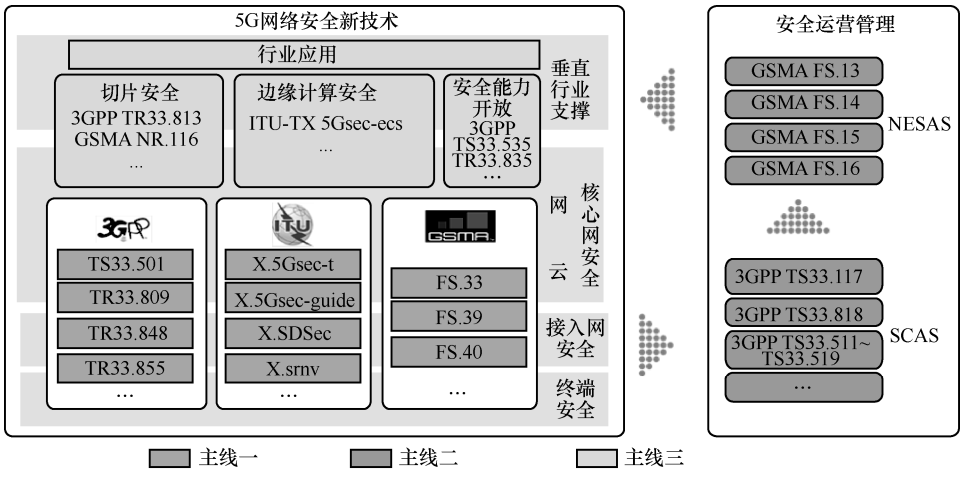

图 2　5G 网络安全新技术与标准 3 条主线

4.1 接入网安全机制演进

在 3GPP 中，定义用户域网络之间的连接为“接入网”，并将与接入相关的安全能力划分到接入域安全。用户接入是涉及设备类型最多、设备数量最多、交互流程最复杂的场景，为了保障用户和网络的安全性，接入域需要有大量的安全保护措施，包括为确保合法终端接入合法网络的认证机制、用户身份保护机制、信令和用户数据安全传输的算法与协议、密码算法协商机制、密钥衍生体系等。

与 4G 相比，5G 网络充分考虑了多类型终端的认证需求、数据安全保护的需求，在接入域进行了大量安全机制增强，主要包括 AKA 机制增强、EAP 框架支持、SUPI 隐私保护、用户数据防篡改等。

4.1.1 5G AKA 认证避免内部攻击

在 4G 网络中，用户接入认证的算法是 EPS-AKA[12]，是一种双向认证机制，用户认证流程中网络与终端的双向真实性得到了有效保障，避免了伪终端/伪网络，经过实践检验是相对安全的。在该机制的设计中，网络被视为一个整体，归属网络将用户认证向量全量发送给漫游网络，并由漫游网络确认用户是否合法，然后反馈给归属网络。EPS-AKA 机制并没有考虑运营商网络内部的攻击问题，可能会存在漫游地运营商欺骗归属地运营商的风险，即漫游地运营商可能仿冒合法用户发起业务请求，获取归属地运营商发送的全量认证信息后，跳过用户与网络双向认证过程，利用全量认证信息仿冒用户回复，即可冒充用户正常使用业务。

5G 安全设计的基础是网络处于一个完全开放与非信任的环境中，为了避免运营商内部/之间欺骗的风险，5G 网络对 4G 中使用的 AKA 协议（在 4G 中被称为 EPS-AKA）做了进一步增强，形成了 5G-AKA 认证机制[4]，对其中重点环节进行描述，5G-AKA 安全机制如图 3 所示。

在 5G-AKA 认证过程中，归属地运营商仅将认证向量的一部分（RAND，HXRES*，…）发送给拜访地运营商，其中关键的是拜访地运营商获得的是认证校验信息（XRES*）的 Hash 值，而不是全量信息。而在认证响应中，用户验证通过后才将全量认证信息发送给拜访地运营商，其中包括 RES*；拜访地运营商对 RES*进行 Hash 后与 HXRES*对比，能有效完成用户校验。校验通过后，拜访地运营商需要将包含 RES*的全量认证信息反馈给归属地运营商，经归属地运营商认证后才能完成整个认证流程。

因此，5G-AKA 的使用有效避免了拜访网络欺骗归属网络的内部攻击行为，避免了拜访网络虚报用户漫游状态等情况的发生。

4.1.2 EAP 认证框架实现认证能力融合

在 4G 网络中，考虑了基于 WLAN 接入的兼容能力并支持对非蜂窝网络的接入采用 EAP（extensible authentication protocol）认证方式，但认证流程与网元仍然是相对独立的，在架构上设立一个独立于 AKA 认证的网元（如 AAA 服务器）来支持。5G 网络的设计更加开放，支持更多类型的终端接入，需要将蜂窝接入、非蜂窝接入的能

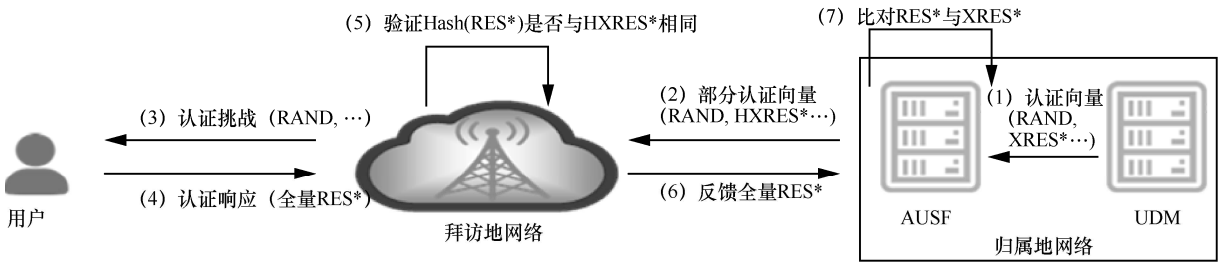

图 3 5G-AKA 安全机制

力整合，因此原来面向蜂窝系统设计的认证机制不再通用。

5G 采用了统一的认证框架，即各种接入方式可以用一套认证体来支持。5G 引入了 EAP 认证框架，支持将 EAP-AKA’[8]作为 5G 网络的必选认证方法，从而实现蜂窝接入与非蜂窝接入的统一接入认证机制。5G-AKA 和 IAP-AKA’的流程与网元完全一致，仅在认证中使用的算法、认证向量的产生不同。因此，“统一”一方面体现在 3GPP 接入，即在使用 5G 无线网接入的时候，也可以采用 EAP-AKA’认证方式。因此，EAP-AKA’认证方式提升到了和 5G-AKA 并列的位置；另一方面，EAP-AKA’认证和 5G-AKA 认证在网络架构上使用了同样的网元，意味着 5G 的认证网元在标准上同时支持这两种认证方式。这样，在 5G 网络中，无论是通过蜂窝网还是非蜂窝网的接入都能基于 EAP 框架进行认证，为垂直行业使用原有的认证方式接入 5G 提供了便利。

4.1.3　基于证书实现用户身份信息保护

在移动通信网中，每个用户都有一个用户永久身份标识，在 2G/3G/4G 时被叫作 IMSI。虽然该信息与用户手机号的对应关系并不公开，但如果该身份信息在空口暴露，仍然有可能对固定用户进行位置跟踪等，从而侵犯用户隐私。在 2G 至 4G 网络中，为了对 IMSI 进行保护，引入了 TMSI。一旦用户入网，则由网络分配的 TMSI 替代 IMSI 在空口传输与使用，避免攻击者监听用户标识，并进一步构造攻击或追踪用户。但是，使用 TMSI 代替 IMSI 在空口上传输仅可以解决大部分情况下的用户隐私保护问题，在少部分终端或网络侧没有 TMSI 的情况下，比如当用户开机第一次接入网络时，或网络侧由于某些原因删除了保存的 TMSI（如用户很长一段时间与网络失去联系）等场景，终端则不得不使用 IMSI 接入网络。

针对上述特定场景下 IMSI 暴露引发用户隐私保护的问题，5G 系统中引入了基于公钥体系的加密机制，对 SUPI 进行加密形成 SUCI，在空口中传递 SUCI 以全面保证用户的隐私在空口不泄露[4]。为支持 SUCI 的计算，首先 SIM 卡需在生产过程中预置运营商公钥，需采用安全方式（如专线、VPN 等方式）将公钥数据传输给供卡商制卡；在用户开机登网等场景下，需要传递 SUPI 时，通过 SIM 卡中的归属网络公钥对 SUPI 进行加密生成密文 SUCI 用于在空口中传输，从而更加有效地保护用户的隐私。在产生 SUCI 时，需要利用 USIM 中预置的归属运营商公钥、采用 ECIES（elliptic curve integrate encrypt scheme）对 SUPI 进行加密运算，并且根据算法原理，每次使用时产生的 SUCI 也不相同。因此攻击者无法根据 SUCI 推算出 SUPI，也无法利用 SUCI 长时间对用户进行探测，进而无法针对用户进行持续性的跟踪。

在 5G 网络中，用户开机登录的过程中 SUCI 和 SUPI 的转换过程如图 4 所示。

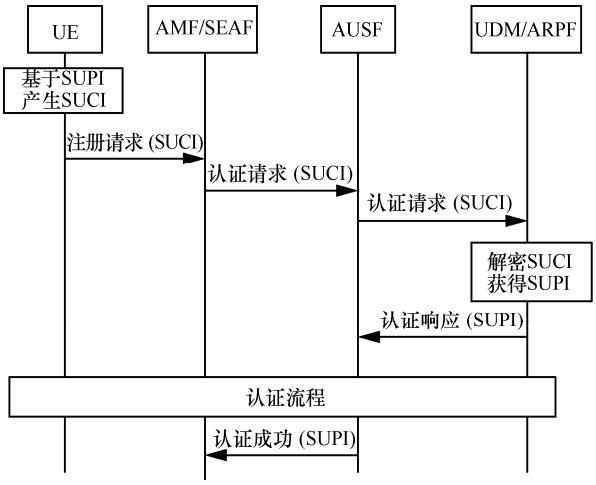

图 4　用户身份标识的加解密机制

4.1.4　数据防篡改能力进一步增强

4G 网络中，已经强制要求对所有信令进行了完整性保护，但考虑到普通用户对数据通道的完整性保护并没有强烈需求，在衡量安全性和业务便利性之后，4G 仍然没有引入数据完整性保护的能力。2018 年，由于业内出现了对用户面数据进

行篡改的理论攻击方法——aLTEr[6]，虽然实施的代价较高，但仍然表明用户面数据缺乏完整性保护时存在一定的风险。

在 5G 时代，一方面考虑到上述风险，另一方面，由于 5G 的设计重点之一是要面向垂直行业提供服务，而与用户语音或上网等业务不同，垂直行业对数据防篡改的需求大大提升，尤其在物联网、工业互联网等场景中，1 个字节的篡改就可能导致生产故障，进而造成巨大损失。因此，5G 网络在空口为用户面数据增加了完整性保护功能。由于用户数据完整性保护会对终端以及无线基站的性能和能耗带来巨大的挑战，所以受限于终端厂商的产品支持能力，在 5G 一阶段即 R15 版本的标准[13]中，仅支持面向低速场景（用户数据传输速率在 64 kbit/s 以下）提供必须的完整性保护，而针对高速场景则不做强制要求。但随着运营商的推动，在 R16 版本的标准[4]中，实现了对所有速率的传输场景均要求强制支持对用户数据的完整性保护。

完整性算法的输入参数包括一个名为 KEY 的 128 位完整性密钥、一个 32 位 COUNT、一个称为 BEARER 的 5 位承载标识、1 位传输方向（DIRECTION）以及消息本身，即 MESSAGE。基于这些输入参数，发送方使用完整性算法 NIA（包含 AES、SNOE 3G、ZUC）计算一个 32 位消息认证码（MAC-I/NAS-MAC）。然后，在发送消息时将消息验证代码附加到消息中。对于完整性保护算法，接收方对接收到的消息计算预期消息认证码（XMAC-I/XNAS-MAC），其方式与发送方对发送的消息计算其消息认证码相同，并通过将其与接收到的消息认证码（即 MAC-I/NAS-MAC）进行比较来验证消息的数据完整性。如何使用完整性算法 NIA 验证消息的完整性如图 5 所示。

4.1.5 双连接的安全保障

uRLLC 是 5G 的三大应用场景之一，可广泛应用于工业控制、智能电网、车联网通信、远程手术等应用场景。5G 网络中设计了双连接架构保障 uRLLC 的高可靠性、低时延等特性，信道的安全、数据一致性保障是其中的关键。

在 uRLLC 冗余传输架构中，主数据通道和冗余数据通道的同步配合确保了用户数据传输的高可靠性，但是如果针对两条数据通道使用同样的密钥进行安全保护，则攻击者很容易识别出两条相同的数据链路从而进行相互关联。这样，攻击者实现对一条数据通道的攻破便可轻易破坏另一条，进而破坏了高可靠传输的“双保障”。3GPP TS33.825[14]标准中设计了双密钥的高可靠保护机制，一方面防止攻击者关联相同数据链路；另一方面防止一条冗余数据通道无安全保护而导致另一条冗余数据通道的安全保护失效。主基站根据安全策略决定辅基站使用的安全保护方法，并发送选择的安全保护方法给辅基站，以使得双连接的安全保护策略（包含完整性保护和机密性保护策略）保持一致，以确保两条数据通道的安全不被降级。双连接的安全保护机制示意图如图 6 所示。

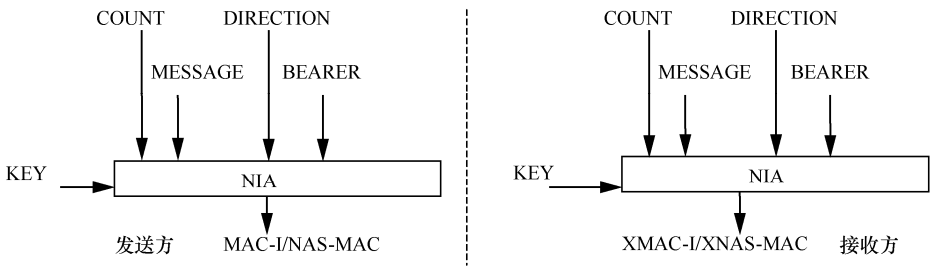

图 5 消息认证码的推衍

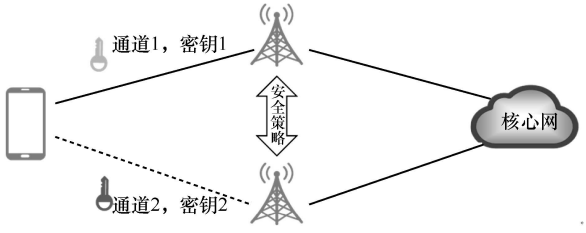

图 6　uRLLC 双连接安全保护机制

4.2　核心网安全机制演进

移动通信网络是由基站和多种类型的核心网络设备构成的复杂网络系统，在基站与基站间、基站与核心网机房间以及核心网机房之间通过各种类型的通信线路连接在一起组成了通信网络系统。这些通信线路，可能是专门建设的，也有可能是与其他线路共同使用的，甚至还有可能是直接借助于互联网线路进行传输的。因此，为了保障信令和用户数据在上述通信线路上的传输，从 2G 开始，就逐渐形成了基于 IP 的网络域安全标准 TS33.210[15]，而且一直并默认运营商间的通信是可信赖的。但随着 5G 网络形态向着虚拟化、云化的方向发展，网络域安全也需要考虑打破域的边界，在开放、非信任的前提下考虑安全机制设计，因此引入了对基于 IP 的网络域安全防护增强、运营商间互联互通安全等安全能力。

4.2.1　基于 TLS 增强设备间安全防护增强

在 2G 到 4G 的 IP 化网络域建设中，将通信网络系统按设备部署方式和外部安全环境划分成不同的网络域，将域内设备间的通信链路视为可信的，而不同的网络域之间传递的信令和用户数据则面临风险，需要在域间基于 IP 地址进行加密和完整性等安全保护[15]。

但随着 5G 通信网络架构的演变，网络功能的虚拟化使得网络节点与 IP 地址的对应关系弱化，使用基于 IP 地址的保护方式不再适用。而且，随着 5G 接入基站部署环境更加多样，部署数量更加庞大，使得网络域划分更加复杂，IPSec 隧道数量将显著增加，因此配置 IPSec 隧道将是一个巨大的挑战。而基站的灵活部署，也会给 IPSec 的管理带来更多的困难。

为了适应更加灵活的网元节点部署，5G 在传统安全防护基础上，增加了新的安全防护机制；即在基站与核心网之间，以及基站与基站之间新增了基于会话层协议的 TLS 安全保护机制[4]。基于 TLS 的保护机制建立在 IP 网络之上的传输层，对 5G 云化网络、虚拟化设备的安全保障提供了新的手段。

4.2.2　SBA 域安全

5G 服务化架构将网络架构由传统的接口型架构演变为总线型的网络架构，将传统网络的接口连接变成服务连接，并引入了新的注册、发现等机制，使提供服务的网络功能允许任意其他网络功能通过服务调用方式获取信息。

总线型的网络架构和开放的服务接口使得任意网络功能均有可能请求访问任意服务，而无论该网络功能是否需要访问该服务。因此，服务化架构增加了网元的暴露面，需要在网络功能发现、服务请求时等关键环节中增强访问控制与授权防护。

一方面，3GPP TS33.501[4]定义了基于静态策略的访问控制能力以及基于 OAuth2.0 的授权与访问控制机制，就可以使提供服务的网络功能（NF provider）在请求服务的网络功能（NF consumer）请求访问服务时验证该 NF consumer 是否有权访问该服务。

另一方面，授权机制需要以确认网络功能的身份为前提，并需要网络能够保障网络功能间的信息传输安全，避免遭受网络功能被假冒，通信信令被窃听、篡改和伪造等问题。考虑到 5G 核心网服务化架构基于 HTTP 提供信令传输，而业界通常使用 TLS 协议为 HTTP/2 传输提供安全保护，因此 5G 网络也遵循这一原则，引入 TLS 机制为网络功能提供身份确认以及网络功能间的安全传输。

4.3　互联互通安全保障

在 2G/3G/4G 网络中，当用户漫游时，拜访地运营商与归属地运营商之间的信令传输没有统一

的标准保护机制。这是因为早期网络建设时，运营商之间的网络采用专线方式，安全性可以通过物理防护等手段保证。但随着网络规模的扩大，运营商之间网络连接变得越来越复杂，网络连接的暴露风险越来越高，并且出现了借助于运营商间网络连接对中转信令进行攻击的情况。

5G 系统为保护运营商之间的信令安全，引入了网络功能 SEPP[4]，并与之同时引入了应用层安全保护机制，在拜访地运营商 SEPP 和归属地运营商 SEPP 之间对信令消息提供应用层协议上的加密和完整性保护，并允许合法的中转运营商在消息后附加具有签名的消息修改信息，基于 SEPP 的域间信令安全框架如图 7 所示。这种机制，一方面保证了运营商间互联互通信令的安全；另一方面也为 IPX 在传输层面基于路由和业务处理考虑对信令的修改提供了空间[4,16]。

4.4 云和虚拟化安全

虽然 3GPP、ITU 标准中都都没有明确建议 5G 网络基于云和虚拟化平台构建，但考虑到 IT 技术的发展趋势、云计算技术的成熟度、垂直行业定制化业务等，国内外主流运营商普遍选择在云基础设施上部署 5G 网络。

5G 系统在网元自身和网络连接两方面引入了虚拟化技术，其中 NFV（network functions virtualization，网络功能虚拟化）[17]实现了计算资源的按需部署和弹性扩缩容以及网元、网络功能的虚拟化；SDN（software defined networking，软件定义网络）[18]实现了网络连接的虚拟化，更有效、更智能化地管理网络拓扑和路由，支持按需配置网络路由和调度流量。与设备厂商提供硬件、软件一体化解决方案相比，云和虚拟化技术的应用为电信网注入了通用化、软件化、可编程等新特性，也为 5G 网络提供用户可定制的能力（如切片服务）以及按需部署打好了基础。

同时，这些变化带来的安全新挑战包括：一方面，存在虚拟化平台和软件自身安全的挑战；另一方面，云化带来的动态性使网络边界模糊，传统依靠物理隔离、部署安全手段的纵深防御体系不再适用。因此，在 3GPP R16 中，启动了专门的项目对虚拟化安全进行研究，主要包括虚拟化对 5G 系统的影响（TR33.848）[19]、虚拟化设备安全保障（TR33.818）[20]等项目。电信云安全体系从云基础设施安全、网络功能安全、业务安全、安全管控 4 个层面构建，尤其是基础设施、网络

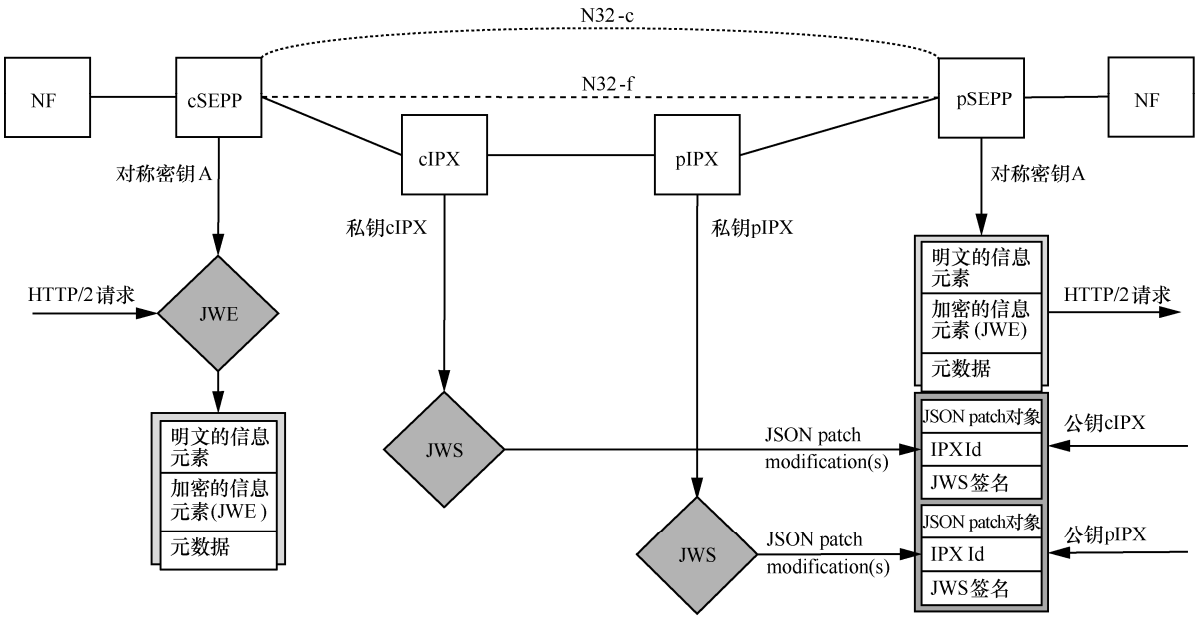

图 7 基于 SEPP 的域间信令安全框架

功能安全与 5G 密切相关。其中虚拟计算资源安全、虚拟网络资源安全、编排与控制安全是电信云基础设施特有的安全要求；网络功能安全主要包括网元间通信协议安全、网元软件安全以及网元自身存储和处理的数据安全。

5　5G 安全服务垂直行业

5G 网络的重要新增应用场景是与垂直行业密切相关的，包括政府、能源、金融、交通、医疗等。相对于个人用户市场，垂直行业通常对网络的安全功能、安全服务和安全保障都有定制化要求。在业务的驱动下，以及在虚拟化和云计算技术的支持下，网络切片、移动边缘计算两项新技术应运而生。

5.1　切片安全

5G 系统设计和实现了端到端网络切片机制，可基于一套物理的 5G 网络虚拟出多个逻辑子网；每个端到端切片由切片无线子网、切片传输子网、切片核心子网组合而成。切片的本质特征在于差异化，包括差异化的部署模式、业务质量、安全等级等，安全性也是切片作为开拓行业用户市场的关键因素之一。网络切片在逻辑上是“独立使用的专网”，但从物理资源角度看，网络切片之间共享物理资源和基础设施。每个切片以“租户”的形式按需使用这些资源；通过切片管理系统的编排、调度和配置实现网络资源灵活分配、网络能力按需组合、网络特性按需定制[21]。

从网络构成来看，切片存在的安全风险如下。

- 无线空口：一是终端从空口接入非授权切片，二是其他终端或信号设备从空口发起大量连接攻击无线设备/用户终端、或冒用其他终端向网络侧发起请求造成攻击等。
- 传输网：数据传输保护不当，导致数据被中间设备明文解析或恶意篡改。
- 核心网：与业务平台的隔离、防护不完善。

从切片的自身构建关键技术来看，存在的安全风险如下。

- 物理资源：服务器（CPU、内存、磁盘、网卡的隔离）等物理设备未能正确划分与隔离，导致数据泄露、数据篡改、资源侵占。
- 虚拟化资源：NFV 中 Hypervisor 的安全缺陷被利用、虚拟机/容器间资源隔离失败，导致切片间相互干扰、虚拟机/容器逃逸、镜像被篡改等；SDN 控制层的安全会影响切片乃至整个网络的安全。
- 切片管理：一方面，网络切片本身的技术复杂性给管理带来的难度远高于传统网络；另一方面，切片管理过程自身也面临误操作、错误配置、配置被篡改等安全风险。

为了保证切片的安全性，在 5G 网络的安全基础架构上，对切片的接入认证、切片的隔离和安全管理等机制可以使 5G 网络切片从基因上具有更强的安全性和灵活性。3GPP 在 R15 和 R16 标准中制订了切片的安全要求，主要包括切片安全隔离、切片认证、切片标识 NSSAI 隐私保护、切片管理安全等。

（1）切片隔离

根据网络建设的不同，同一个切片中的网元可能位于不同的数据中心，形成分布式系统。需要基于安全隔离要求编排网元和组网方式，从而保证切片安全性符合行业客户预期。

跨数据中心的物理通信链路需要承载多个切片的业务数据传输，需要通过策略路由、SDN、VxLAN、IPSec VPN（virtual private network）等诸多技术实现不同切片间通信的隔离。同样，在数据中心内部，也可采用上述机制保证不同切片之间、同一主机内部不同切片的网元之间的隔离。此外，同一个切片内不同网元也有不同的安全保护级别，比如用于用户数据管理的 UDM 的安全

级别应高于用于接入管理的 AMF，因此不同安全级别的网元之间也需要进行隔离。

针对切片可建立三级立体化安全隔离体系，包括切片间隔离、切片网络与用户隔离、切片内网元间隔离[22]。

首先是切片间隔离。5G 网络承载多种不同安全特性的网络切片，如一般性的娱乐服务、高安全诉求的金融服务、低时延高可靠的工业控制服务等。应该依据垂直行业业务和数据资产的重要性，进行切片间的有效隔离，保障每个切片具有对应安全级别。其中，回传网络可以基于 SPN 实现 SPN 软隔离、FlexE 硬隔离两种手段；核心网网元可以通过逻辑（虚拟机）隔离、物理（物理机）隔离两类。

其次是切片网络与用户隔离。为保障 5G 网络切片的安全、高可靠运行，在切片网络设计时，需要在最终用户侧、垂直行业应用侧设置隔离机制，并通过切片接入的环节保证仅有允许的用户能接入切片，保证切片网络自身安全边界清晰，确保切片网络自身的安全可控。

最后是切片内网元间隔离。网络切片内隔离主要有两种方式：一是切片内不同网元具有不同的安全级别和对外服务接口，需要根据网元的安全级别要求，在切片网内划分出安全域，提供网元间安全隔离；二是切片网络结构支持移动边缘计算架构时，需要保障移动边缘计算服务器与核心网网元之间的安全域隔离。

（2）切片认证

切片认证机制是为了进一步加强行业客户对接入切片用户的安全控制和自主管理而引入的。如果一个网络切片要求终端在接入切片前需要进行切片接入认证，那么在 5G 网络主认证完成后，终端需要使用针对该切片的身份标识和认证凭据、EAP 与切片 AAA 服务器开展切片认证，保证只有获得授权的终端才能找到并合法接入切片网络。这项机制防止了来自非授权用户对切片网络资源的消耗和可能发起的对切片网络的攻击，从而提升了切片网络的可用性和行业客户对用户的可控性[14]。

为了让合法的终端接入和使用切片，3GPP 设计了网络切片选择辅助信息（network slice selection assistance information，NSSAI）。一方面，合法终端需要正确配置网络切片标识和切片业务标识才能访问和使用切片资源，在用户初始接入网络时，NSSAI 指示基站及核心网网元将其路由到正确的切片网元；另一方面，NSSAI 对于垂直行业属于敏感信息，5G 网络可对 NSSAI 进行隐私保护。

（3）切片安全管理

除了上述切片本身的安全机制之外，还需要对切片运行状态、切片生命周期管理和维护安全进行管理[4]。切片的管理安全包括两个部分，一是通过管理手段保证切片的可用性；二是保证切片管理过程的安全。

针对切片的可用性，提供实时的切片安全监控能力、应急处置以及故障恢复能力，实时掌握切片的运行情况、可能的被攻击情况及故障状况，通过联动对应的安全设备进行处置，并及时对故障进行修复，从而保障系统的可用性。

针对切片管理的安全，一方面，切片管理服务使用方调用切片管理服务提供方提供的服务进行切片管理，为了保障切片管理的安全，要设置相应的安全保护机制[22]，包括切片管理服务使用双向认证、授权机制，切片管理系统及切片网络间通信需做完整性、机密性保护以及防重放攻击。另一方面，在切片生命周期管理中，切片模板、配置需要具备检查与校验机制，避免错误模板、错误人工配置导致切片的访问控制失效、数据传输与存储存在安全风险等；切片去激活或终止后，遵照数据隔离要求做好数据清除工作。

5.2 移动边缘计算安全

移动边缘计算（mobile edge computing，MEC）

技术通过在靠近用户侧部署 IT 资源，提供处理、存储、通信能力，使得接入网具备了业务本地化部署的条件，从而提供了高带宽、低时延的传输和业务就近处理能力。同时，业务面下沉到本地化部署，可以有效降低对网络回传带宽、时延要求和网络负荷。

一方面，移动边缘计算作为 5G 网络架构下云计算技术的延伸和补充，提供了业务和网络安全的增强机制。首先，针对有高等级信息安全要求的垂直行业应用（如工业控制、智慧医疗），用户的业务流量可以直接分流到移动边缘计算平台，并在本地化进行业务处理，保证数据不出园区；其次，移动边缘计算平台作为最靠近用户侧的 IT 资源平台，可部署安全功能（如 DPI、防火墙、抗 DoS 和流量清洗等）对终端进行行为分析、流量管控，实现终端安全防护和近源安全治理，在物联网、工业互联网等场景中，在不改造终端的前提下增强系统安全。

另一方面，移动边缘计算带来网络架构和业务处理方式的变化，引入了新的安全风险。具体包括移动边缘计算分流使用的核心网 UPF 下沉到边缘，使运营商的核心网边界下移，UPF 可能受到物理攻击进而给核心网带来安全风险，比如，以边缘 UPF 为跳板对核心网设备形成攻击；移动边缘计算平台自身的安全需要增强；此外，移动边缘计算平台是电信云的延伸，NFV 的安全威胁同样适用于 MEC。

此外，在移动边缘计算的设计、业务部署和实施中，除了考虑物理安全、基础设施安全、组网安全、安全管理外，还应考虑 MEC 平台安全、应用安全、UPF 安全以及 MEC 编排和管理安全。

5.3　AKMA 安全能力开放

传统通信网络重点为用户提供语音和数据通信服务，网络本身所具有的能力并不作为主要业务对外开放。但 5G 网络为了更好地满足各垂直行业的个性化需求，通过能力开放将运营商的网络能力及安全能力开放给第三方应用。这样一来，不仅可以及时响应行业业务需求，提供个性化的服务及安全保障，也可以将运营商的能力最大化利用。

在 5G 大规模物联网部署的场景中，应用提供方在大量终端的认证和初始安全凭证的配置管理上面临着成本高、密钥分发安全性低的问题。为了帮助垂直行业尤其是物联网应用提供商解决这个问题，5G 引入了一项新的安全机制——AKMA[9,23]，制订了一套流程简化、轻量级的、可适配多种物联网场景的应用层认证和密钥管理架构及流程，可以利用终端与网络的认证结果，进一步为应用层提供身份认证和会话密钥管理服务，避免了应用层大规模的产生和分发初始密钥时密钥泄露所带来的安全问题。

在 3GPP TS33.535 中，引入新定义的网元——AAnF（AKMA anchor function，AKMA 服务的锚点网元）实现了安全服务能力，AKMA 锚点网元 AAnF 如图 8 所示。当用户终端成功接入 5G 网络之后，用户终端和网络侧的 AUSF 中同时生成了主密钥 K_{AUSF}，AAnF 利用了 K_{AUSF} 可以用于进一步衍生各类密钥的能力。如果终端注册并签约了 AKMA 服务，那么在初始认证完成之后，终端和 AUSF 就会相应地生成 AKMA 中间密钥 K_{AKMA} 及对应的密钥标识符，向应用服务器（第三方）提供后续会话密钥。随后，终端向应用服务器发起业务请求时，在请求消息中会携带密钥标识符，当应用服务器收到该请求时，会带着该密钥标识符向 AAnF 请求会话密钥。AAnF 根据从 AUSF 处获取的 AKMA 中间密钥（K_{AKMA}）推衍出会话密钥（K_{AF}），并返回给应用服务器。终端在收到应用服务器返回给自己的应用层响应消息后，也根据自身存储的 K_{AKMA} 推衍出会话密钥 K_{AF}。这样，应用服务器和终端即可使用该会话密钥进行后续的应用层认证或数据加密等。

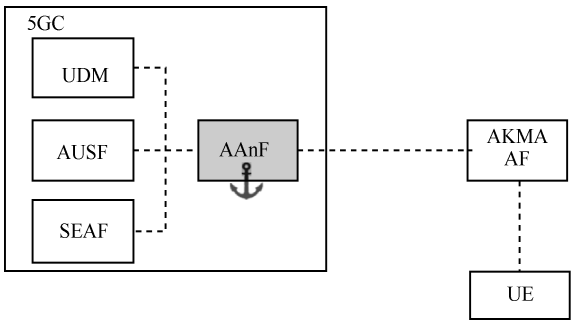

图 8　AKMA 锚点网元 AAnF

6　5G 网络安全测评体系

移动通信系统的安全除了需要设计安全的架构、机制、流程和协议之外，还需要确保安全设计真正被落实，因此，对网络设备的安全评估和测试至关重要。网络设备的安全功能和接口协议已由 3GPP 制订，而网络设备自身的安全要求、安全评估等缺乏相应的标准与实施流程。以前的 3GPP 标准只规定了安全功能和接口协议，设备安全配置等需要行业、企业标准去规范，带来定制化的成本；而相关安全要求制订时缺乏必要依据，使得安全要求只能来自于现网运营的最佳实践，存在风险覆盖不全面的可能性。

在这样的背景下，3GPP SCAS（security assurance specification）和 GSMA NESAS（network equipment security assurance scheme）应运而生。

6.1　测评标准体系的形成

目前国际上最主要的安全测评体系是通用准则（common criteria，CC）[24]，可对系统的实现能力进行审计与认证。3GPP TR33.805[25]分析了 3GPP 网络产品安全评估的方法论的问题，认为 CC 中的分级是对不同评估范畴、不同评估深度和不同评估技术手段的包装，在 CC 中评估等级从 EAL2 到 EAL4，不同的等级刻画了安全评估的实施程度和安全保障的不同的均衡点。3GPP 认为 3GPP 网络产品的评估范畴、评估深度应该是比较确定的，所以不需要 CC 那样的评估等级，也不需要 CC 的证书许可过程。

3GPP 定义的安全保障方法论（SECAM）[21]明确：由 3GPP 制订安全保障相关的安全要求、测试方法相关标准；由 GSMA 制订认证流程、产品开发过程的安全性审核以及测试实验室资质相关的标准。3GPP 和 GSMA 的相关标准的关联关系如图 9 所示。

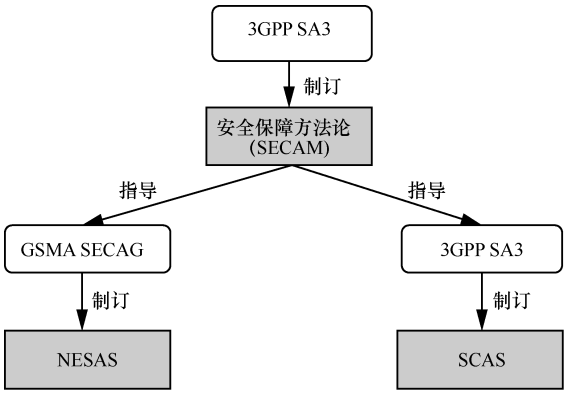

图 9　3GPP 和 GSMA 安全测评标准的关联关系

6.2　3GPP SCAS 评估规范体系

3GPP TR33.916[26]基于 TR33.805 确定的方法论技术路线，对方法论的具体落实进行描述。包括如何撰写一个网络产品的 SCAS 文档，分哪些步骤，安全描述、测试用例必须包含哪些内容，评估应该由哪些步骤组成，参与者分别承担什么角色等。

SCAS 的方法论包括：

- 安全测评建立在网络产品威胁分析的基础上；
- 对于每一类网络产品采用单一的安全基线和单一的安全评估等级；
- SCAS 的评估分为安全一致性测试、基本的渗透测试和增强的渗透测试。

从安全的视角看，网络产品虽然功能不同，但在安全威胁和安全评估上是有共性的，这些共性可以形成一些安全评估的最小集。3GPP TR33.926[27]对网络产品的分类、所面临的安全风险、需要保护的关键资产等进行了识别和描述。从安全评估的视角来看待网络产品，一个比较粗粒度的模型如图 10 所示。

图 10　网络设备通用模型

基于这个模型来观察网络产品上的关键资产，主要的安全评估要点包括用户账户数据和安全凭证；日志数据；配置数据，如网络产品的 IP 地址、端口、VPN ID、管理对象（如用户组、命令组）；操作系统（如操作系统上的文件和进程）；网络产品上的应用程序；充足的处理能力，即处理能力未被消耗到极限；硬件（如主机、单板、供电单元；接口）；操作台配置口；OAM 接口等。这些通用的评估形成了 1 册通用的安全规范——3GPP TS33.117[28]，而针对不同设备的增量部分则形成了若干本 5G 设备安全规范[29-37]，归纳见表 2。

6.3　GSMA NESAS 安全保障框架

GSMA 则制订了 NESAS，包括网络设备的产品开发流程与生命周期管理流程的安全审计、安全测试实验室的认证和网络设备安全评估 3 个部

表 2　3GPP SCAS 文档

	安全测评方法论	
TR33.805	Study on security assurance methodology for 3GPP network products	网络产品安全保障方法研究与选择
TR33.916	Security assurance methodology (SCAS) for 3GPP network products	网络产品安全保障方法论
TR33.926	Security assurance specification (SCAS) threats and critical assets in 3GPP network product classes	3GPP 网元产品威胁和重要资产
	通用安全要求	
TS33.117	Catalogue of general security assurance requirements	网络产品通用安全保障要求及测试用例
	5G 设备特定安全要求	
TS33.511	5G security assurance specification; NR node B (gNB) network product class	5G 基站 gNB 安全评估标准
TS33.512	5G security assurance specification; access and mobility management function (AMF) network product class	AMF 网元（接入鉴权和移动性管理控制功能）安全评估标准
TS33.513	5G security assurance specification; user plane function (UPF) network product class	UPF 网元（用户面功能，执行用户面数据转发等功能）安全评估标准
TS33.514	5G security assurance specification for the unified data management (UDM) network product class	UDM 网元（统一数据库，存放用户的签约数据等）安全评估标准
TS33.515	5G security assurance specification; session management function (SMF) network product class	SMF 网元（会话管理网络功能）安全评估标准
TS33.516	5G security assurance specification; authentication server function (AUSF) network product class	AUSF 网元（鉴权网络功能）安全评估标准
TS33.517	5G security assurance specification for the security edge protection proxy (SEPP) network product class	SEPP 网元(安全代理，漫游场景下链接 HPLMN 和 VPLMN）安全评估标准
TS33.518	5G security assurance specification for the network repository function (NRF) network product class	NRF 网元（服务注册、发现、授权等功能）安全评估标准
TS33.519	5G security assurance specification for the network exposure function (NEF) network product class	NEF 网元（对外开放网络能力和服务）安全评估标准

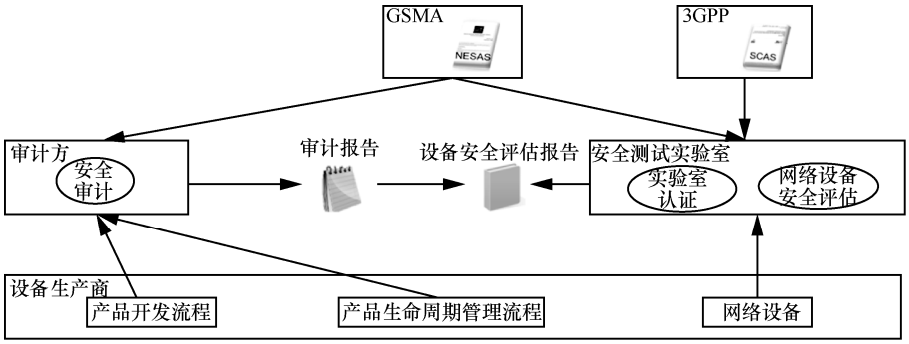

图 11　NESAS 测评的执行过程

分，其中安全评估部分使用 3GPP SCAS 作为测试规范，其过程如图 11 所示。

NESAS 保障框架对以审计评估和测试评估两种方法都支持。NESAS 制订了审计评估的系列文档，并引用 3GPP 制订的 SCAS 系列规范作为测试评估的要求。NESAS 的文档结构如图 12 所示。

2019 年 11 月 GSMA 发布了第一版 NESAS 标准[38-42]，NESAS 的目标是通过制订业界认同的安全基线，为设备厂商和运营商提供安全保证。作为业界第一套针对电信设备的安全评估体系、流程和标准化基线，它解决了运营商制订设备安全要求时缺乏依据的问题和定制化成本高的问题；同时也有助于降低各个国家和地区的管制要求差异以及运营商的需求差异所导致的安全需求的碎片化，降低了厂商的额外开销。

其中，FS.15 Network Equipment Security Assurance Scheme-Product Development and Life-cycle Accreditation Methodology[40]定义了对过程进行认可（accreditation）的方法论，描述了执行审计和认证的过程。FS.16 Network Equipment Security Assurance Scheme-Vendor Development and Product Lifecycle Security Requirements[41]定义了厂商为了获得认可需要满足的需求，独立审计团队根据这些需求来对厂商进行评估。

审计需求中，对资产、威胁、安全对象、需求等进行了定义，在目前的版本中资产描述 7 项，威胁描述 15 项，安全对象 14 项，安全需求 20 项，具体见表 3。

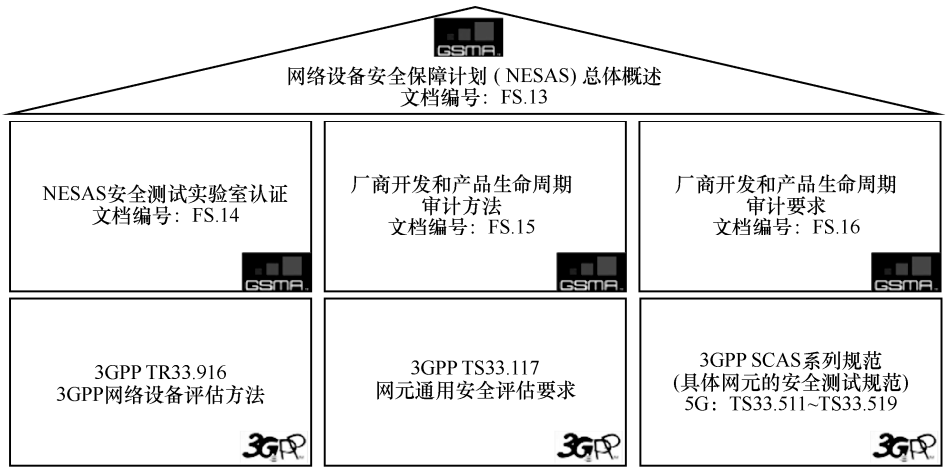

图 12　GSMA NESAS 文档族结构

表 3　厂商开发过程和产品生命周期的安全需求

资产	威胁	安全对象	需求
• 源代码 • 软件包 • 成品 • 安全文件 • 在运营的产品 • 产品开发支持系统	• 流氓开发者 • 源代码漏洞 • 第三方代码漏洞 • 安全设计缺陷 • 非正版发布 • 包含漏洞的老旧版本 • 篡改编译环境 • 错误的文件 • 客户无人负责安全事件处理	• 代码变更控制 • 无漏洞的软件 • 漏洞处理 • 敏感文档不被泄露 • 建立受保护的环境 • 软件完整性保护 • 软件版本识别 • 产品安全修复知识 • 安全设计 • 安全测试 • 员工教育 • 客户文档 • 第三方组件漏洞检测	• 设计安全 • 版本控制安全 • 变更跟踪 • 源代码审查 • 软件安全测试 • 员工教育 • 漏洞修补流程 • 漏洞修补措施独立性 • 信息安全管理系统 • ... • 安全联络点

7　结束语

从 1G 到 5G，移动通信网络与业务不断发展，安全体系也在不断丰富与完善。5G 继承了经过时间和实践验证有效的 4G 安全特性，还对网络自身安全进行了增强，同时还针对更多业务场景的需求扩展了安全能力，形成了更丰富与更完善的安全体系。

7.1　5G 安全发展趋势

（1）5G 安全的重要性仍将不断提升

随着全球 5G 技术的研发和商用步伐进一步加快，5G 安全已成为各国关注的焦点，全球已经形成 5G 网络的安全与国家安全、经济安全以及全球稳定性紧密关联的共识。例如，《美国 5G 安全策略》（National Strategy To Secure 5G of the United States of America）[3]等政策法规，已将 5G 安全提升到国家高度，并将政策法规要求、供应链安全、安全审查等要求加入对 5G 建设的考量中。

（2）5G 安全体系仍将不断演进

5G 网络安全技术体系是基于开放网络环境与业务新需求，并在 4G 的基础上逐渐形成的。但目前 5G 的建设才刚刚起步，未来在 5G 规划、建设、运营的过程中，安全体系与手段的考虑是未来的需求和重点。与此同时，随着 5G 网络的演进并与垂直行业紧密融合，5G 安全的范围还在不断扩展。

（3）5G 安全攻击方法可能持续出现

自 2018 年开始，学术界就开始对 5G 安全风险进行不断分析与挖掘。首先，由于 5G 网络可以和 4G 网络交互，所以针对 4G 网络的风险仍然存在；另一方面，虽然目前没有针对 SA 网络的有效攻击，但随着对 5G 的算法、协议、设备、应用等安全研究工作仍在持续，随着攻击设备发展、计算能力提升，安全威胁可能持续加大，需要密切关注。

7.2　5G 安全工作展望

围绕着开放环境下的安全防护、安全能力与

服务建设两个出发点，如下几方面可能是未来 5G 安全技术工作开展的重点方向。

一是基于“非信任”理念，在更大范围内完善安全技术框架。随着各个国家层面的法规要求的出台、5G 网络建设运维等工作的开展、垂直行业业务的发展等，5G 的生态圈将不断丰富与发展。在此过程中，更需要明确安全责任体系、制订认证评估机制，促进监管方、运营商、设备商等各方形成安全边界共识、明确安全责任、构建协同的工作机制。

二是进一步推动安全技术国际标准制订。在 5G 建设与发展的过程中，国际标准化组织是产业链各方沟通的平台，并最终达成共识完成了统一标准的制订。目前，在 3GPP、ITU 等组织中，5G 安全的重点工作是专网、消息等业务应用的安全，下一步还会涉及数据、能力开放的安全等方面。面向更开放的 5G 网络、更丰富的业务，需要进一步加强安全标准的制订，形成公开、统一的安全要求与体系。

三是进一步研究安全赋能垂直行业。5G 垂直行业方兴未艾，预计在未来的一段时间内都将迅速发展。应该以业务的需求为输入、网络能力为承载，不断将更多、更好的安全能力输出到垂直行业中，为垂直行业提供保障与赋能。

四是关注安全攻防新技术的发展。在 5G 未来的发展过程中，计算能力与攻防技术的提升必将形成新的安全风险和挑战，还需要不断研究并关注安全新漏洞与新风险，制订缓解与修复机制。

相信未来随着 5G 应用的进一步深入普及，5G 网络安全技术也将得到更多的检验与完善，为各行各业的发展提供安全保障。

参考文献：

[1] ITU-R. IMT vision-framework and overall objectives of the future development of IMT for 2020 and beyond: M.2083-0[S]. Geneva: ITU, 2015.

[2] 李正茂, 王晓云, 张同须, 等. 5G+: 5G 如何改变社会[M]. 北京:中信出版社, 2019.
LI Z M, WANG X Y, ZHANG T X, et al. 5G+: how 5G will change society[M]. Beijing: CITIC Publishing House, 2019.

[3] The White House, US. National strategy to secure 5G of the United States of America [S]. 2020.

[4] 3GPP. Security architecture and procedures for 5G system: TS33.501 V16.3.0[S]. 2020.

[5] 3GPP. System architecture for the 5G system: TS23.501 V16.3.0[S]. 2019.

[6] RUPPRECHT D, KOHLS K, HOLZ T, et al. Breaking LTE on layer two[C]//Proceedings of 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019.

[7] 3GPP. Study on enhancements to the service-based architecture: TR23.742 V16.0.1[R]. 2018.

[8] 3GPP. System architecture for the 5G system; stage 2: TS23.501 V16.1.0[S]. 2019.

[9] 3GPP. Authentication and key management for applications (AKMA) based on 3GPP credentials in the 5G system (5GS): TS33.535[S]. 2020.

[10] GSMA. Network equipment security assurance scheme-overview: FS.13 V1.0[S]. 2019.

[11] 3GPP. 3GPP system architecture evolution (SAE)-security architecture: TS33.401 V15.6.0[S]. 2018.

[12] IETF. Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA’): RFC5448[S]. 2009.

[13] 3GPP. Security architecture and procedures for 5G system: TS33.501 V16.0.0[S]. 2019.

[14] 3GPP. Study on the security of ultra-reliable low-latency communication (uRLLC) for the 5G system (5GS): TR33.825[S]. 2020.

[15] 3GPP. Network domain security-IP network layer security: TS33.210 V16.3.0[S]. 2020.

[16] 3GPP. Study on security aspects of the 5G service based architecture (SBA): TR33.855 V1.9.0[R]. 2019.

[17] ETSI. Network functions virtualisation (NFV); architectural framework: GS NFV 002 V1.2.1[S]. 2014.

[18] ONF. Software-defined networking: the new norm for networks[R]. 2012.

[19] 3GPP. Study on security impacts of virtualization in 5G: TR33.848 V0.5.0[R].2020.

[20] 3GPP.Security assurance methodology (SECAM) and security assurance specification: TR33.818 V0.6.0[R]. 2019.

[21] 粟栗, 杨波, 王珂, 等. 面向垂直行业的 5G 网络切片安全白皮书[R]. 2018.
SU L, YANG B, WANG K, et al. 5G network slicing security white paper for vertical industries[R]. 2018.

[22] 3GPP. Study on security aspects of 5G network slicing management: TR33.811[R]. 2019.

[23] 3GPP.Study on authentication and key management for applica-

tions based on 3GPP credential in 5G: TR33.845 V16.1.0[R]. 2019.
[24] ISO/IEC. Common criteria for information technology security evaluation part 1: introduction and general model version 2.3[S]. 2005.
[25] 3GPP. Study on security assurance methodology for 3GPP network products: TR33.805[R]. 2019.
[26] 3GPP. Security assurance methodology (SCAS) for 3GPP network products: TR33.916[R]. 2019.
[27] 3GPP. Security assurance methodology (SCAS) threats and critical assets in 3GPP network product classes: TR33.926[R]. 2019.
[28] 3GPP. Catalogue of general security assurance requirement: TS33.117[S]. 2019.
[29] 3GPP. 5G security assurance specification; NR node B (gNB) network product class: TS33.511[S]. 2019.
[30] 3GPP. 5G security assurance specification; access and mobility management function (AMF) network product class: TS33.512[S]. 2019.
[31] 3GPP. 5G security assurance specification; user plane function (UPF) network product class: TS33.513 [S]. 2019.
[32] 3GPP. 5G security assurance specification for the unified data management (UDM) network product class: TS33.514 [S]. 2019.
[33] 3GPP. 5G security assurance specification; session management function (SMF) network product class: TS33.515 [S]. 2019.
[34] 3GPP. 5G security assurance specification; authentication server function (AUSF) network product class: TS33.516 [S]. 2019.
[35] 3GPP. 5G security assurance specification for the security edge protection proxy (SEPP) network product clas: TS33.517 [S]. 2019.
[36] 3GPP. 5G security assurance specification for the network repository function (NRF) network product class: TS33.518[S]. 2019.
[37] 3GPP. 5G security assurance specification for the network exposure function (NEF) network product class: TS33.519[S]. 2019.
[38] GSMA. Network equipment security assurance scheme- overview: FS.13[S]. 2019.
[39] GSMA. Network equipment security assurance scheme-security test laboratory accreditation requirements and process: FS.14[S]. 2019.
[40] GSMA. Network equipment security assurance scheme-product development and lifecycle accreditation methodology: FS.15[S]. 2019.
[41] GSMA. Network equipment security assurance scheme-vendor development and product lifecycle security requirements: FS.16[S]. 2019.
[42] 杨志强, 粟栗, 杨波, 等. 5G 安全技术与标准[M]. 北京: 人民邮电出版社, 2020.
YANG Z Q, SU L, YANG B, et al. 5G security technologies and standards [M]. Beijing: Posts & Telecom Press, 2020.

[作者简介]

杨志强（1963− ），女，中国移动通信有限公司研究院副院长、教授级高级工程师，享受政府专家津贴，主要从事网络技术、云计算及安全等领域技术和策略研究及标准化等工作。

粟栗（1981− ），男，博士，中国移动通信有限公司研究院安全技术研究所副所长、教授级高级工程师，主要从事移动通信网安全技术研究等工作。

齐旻鹏（1983− ），男，中国移动通信有限公司研究院安全技术研究所高级工程师，主要从事 LTE、5G 等通信网络安全技术研究等工作。

杨波（1973− ），男，博士，中国移动通信有限公司研究院主任研究员、高级工程师，SDN/NFV/AI 标准与产业推进委员会（CCSA TC610）安全组组长，主要从事移动通信网络与业务安全、云安全技术等工作。