移动通信网鉴权认证综述

胡鑫鑫，刘彩霞，刘树新，游伟，乔康
（国家数字交换系统工程技术研究中心，河南 郑州 450001）

摘　要：随着移动通信网技术的演进，网络安全问题日益突出，如何在提供高质量通信服务的同时保护合法用户的隐私不被非法窃取、运营商网络不被入侵成为移动通信安全领域的一个重要问题。用户与网络的相互鉴权是用户和网络彼此判定对方合法性的重要手段，鉴权手段也随着网络演进而不断演进，从历代移动通信网络（GSM、CDMA、UMTS、LTE）鉴权认证技术入手，分析鉴权技术优缺点，并重点剖析了即将商用的第五代（5G）移动通信的鉴权技术、统一认证技术，最后对未来鉴权技术的发展进行了展望。

关键词：移动通信网；鉴权；安全；第五代移动通信；统一认证
中图分类号：TN929
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2018096

Overview of mobile communication network authentication

HU Xinxin, LIU Caixia, LIU Shuxin, YOU Wei, QIAO Kang
National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450001, China

Abstract: With the increasingly serious security situation of mobile communication network, it becomes an important issue about how to protect the privacy of legitimate users while providing high-quality communication services, and how to protect the carrier network from being invaded becomes an important issue in the field of mobile communication security. Authentication is an important means for users and networks to authenticate each other's legitimacy. Authentication methods are also evolving along with network evolution. Starting with the authentication methods of past mobile communication networks (GSM, CDMA, UMTS, LTE), the advantages and disadvantages of each generation of authentication technology are analysed, along with which the authentication technology and unified authentication technology of the fifth-generation (5G) mobile communication to be commercialized are emphatically analysed. In the last, reasonable prospect for the development of authentication technology in the future are proposed.

Key words: mobile network, authentication, security, 5G mobile communication, unified authentication

1　引言

作为国家关键基础设施的一部分，蜂窝移动通信网络不仅影响个人生活方方面面（如导航、上网、通信），同时也影响整个社会（如商业、公共安全信息传播）。因此，移动通信网络经常成为攻击者的攻击目标。一方面，攻击者的攻击目标可能针对用户个人隐私，如窃取用户位置、通话

收稿日期：2018-08-21；**修回日期**：2018-10-20
通信作者：胡鑫鑫，justinhu@hust.edu.cn
基金项目：国家自然科学基金创新研究群体资助项目（No.61521003）；国家重点研究发展基金资助项目（No.2016YFB0801605）
Foundation Items: The National Natural Science Foundation Innovation Group Project of China (No.61521003), The National Key Research and Development Program of China (No.2016YFB0801605)

内容等；另一方面，攻击者的攻击目标可能针对整个国家的移动通信网络，这对一个国家的信息网络安全构成巨大威胁。资源丰富的对手（如国外情报机构、恐怖分子）可以通过利用移动通信网的漏洞造成严重破坏（如用户位置跟踪[1-2]）。为了保证移动通信网的安全和运营商、用户合法权益，鉴权认证机制成为保护移动通信网的第一道防线。

移动通信网通常由 3 部分组成，即核心网（CN，core network）、无线接入网（RAN，radio access network）和用户设备（UE，user equipment）。其中移动用户设备属于用户个人，由用户直接控制，接入网与核心网属于运营商，由运营商直接控制。如果用户希望使用运营商服务和网络资源，需要用户和运营商共同协商，这就涉及鉴权认证，判明和确认通信双方真实身份[3]。简单来说，网络侧需要根据用户设备中存储的身份识别参数判定用户是否合法，校验这些参数的过程就是网络对终端的鉴权认证技术；同样地，如果用户设备需要对网络鉴权，同样需要验证网络所提供的参数。鉴权是一个询问与响应的过程，以保证合法用户才能接入网络，合法网络才能服务用户。

2 移动通信网面临威胁与安全需求

自无线通信系统诞生以来，移动通信网就不断遭受各种安全问题的袭扰。最早的模拟通信系统基本没有采用任何安全技术，直接后果就是安全问题频出，窃听用户通话和运营商网络被盗用现象屡见不鲜。第二代（2G）移动通信技术虽然增加了一些安全措施，但是其安全形势并没有得到根本性改变[4]，在随后的第三代（3G）移动通信、第四代（4G）移动通信技术也都不断被爆出安全问题[5-8]，甚至在刚刚完成第一阶段标准的第五代（5G）移动通信系统，也被分析出实际标准未达到其设想的安全需要的情况[9]。移动通信网必须利用空中无线信道进行信息传输，而该信道是开放的，只要攻击者运行安装合适协议栈的天线就可以接收信息。不仅如此，由于整个空口协议体系异常复杂，出于性能和可用性等考虑，该协议体系可能存在安全漏洞，这就降低了移动通信网的安全性。在智能手机兴起之后，各类应用软件层出不穷，而终端存储着海量用户信息和浏览数据，这些软件很容易受到安全问题的困扰，因此，移动通信网络关乎用户的隐私甚至生命财产安全。具体来说，移动通信网所面临的威胁主要包括以下几个方面。

1) 窃听。无线接入网是移动通信网的根基，它形成了用户和运营商核心网的通路，但这条空中无线信道却由于其开放性而极易被攻击者窃听。一方面，攻击者可以利用空口协议上的漏洞直接获得空口信道上传输的信息，另一方面，窃听者即使不能直接解码消息内容，也可以在获得消息源和目的地址后，通过信道中消息流推测通信内容[10-11]，这种攻击方式通常被称为流量分析。

2) 信息篡改。信息篡改是指攻击者先修改或者删除信息的部分甚至全部内容，然后将修改后的内容发送给信息原本的接收方。移动通信网络中传递的消息需要在核心网和接入网基站之间进行转发，在这个过程中，攻击者也可能篡改信息[12-13]。此外，在无线信道上，攻击者通过设立伪基站使受害者设备附着，然后将伪基站连接合法基站，用户所有消息均经过攻击者设备，攻击者便可以篡改其中传输的用户信息。

3) 假冒攻击。假冒攻击是指攻击者通过一定的技术手段窃取真实用户身份信息，并使用该信息在运营商网络成功注册，进而接入合法网络，随后攻击者在合法网络中以受害者身份活动。在窃取合法用户身份信息时，攻击者首先假冒网络控制中心骗取用户接入，随后运行鉴权协议获取用户的身份信息[14]。

4) 服务后抵赖。服务后抵赖是指交易完成后，交易其中一方否认参与过该交易[15]。

5) 重放攻击。攻击者将截获的正常消息再次发送给信息原本的接收者，尽管情形已经发生变化，攻击者通过一定技术手段使最终结果与信息失效前相同[16-18]。

6) 恶意代码。移动终端需要运行相应的操作系统，倘若攻击者利用操作系统漏洞注入恶意代码，则攻击者可以随意地控制设备而不被用户察觉，甚至有时用户安装的应用软件也会非法获取用户终端权限，用以搜集用户隐私数据或者窃取账号密码[19-20]。

面对以上种种威胁，移动通信网安全研究人员试图通过种种技术手段以提高其安全性，尤其是针对移动用户终端设备和网络之间的鉴权过程，空口数据根据实际网络情况，可以抽象出以下几个方面的安全需求[15]。

1) 用户身份的隐蔽性。在 2G、3G、4G 网络中，每个使用运营商服务的移动终端都有唯一且固定的身份标识——国际移动用户识别号（IMSI，international mobile subscriber identification number），但在有些场景下用户终端以明文消息给网络发送自身 IMSI，若这一性质被攻击者利用就会导致用户 IMSI 被非法获取。

2) 双向鉴权。在 GSM 通信系统中，只有网络对用户的鉴权，而没有用户对网络的鉴权，这导致攻击者可以伪冒运营商网络欺骗合法用户，因此还需要增加用户对网络鉴权，这样才能避免伪基站等非法网络欺骗合法用户。

3) 机密性。以往的移动通信网络往往采用计算复杂度较小的对称加密算法，然而对称加密算法有一个天然缺陷，那就是通信双方在协商完密钥之前必须明文传递信息，这些明文信息经常被攻击者利用。如今，移动终端的计算能力大大提升，足以满足非对称加密算法的计算要求。5G 鉴权认证机制使用了 ECC 非对称加密算法，以防止历代网络中的 IMSI 捕获攻击，此外在 3G、4G、5G 网络中使用的其他加密算法还有 SNOW、AES、ZUC 等[21]。

4) 完整性保护。信息完整性是指系统中信息的完整和真实可信，防止攻击者对系统中数据的非法删除、更改、复制和破坏。攻击者通过中断、窃取、篡改和伪造系统信息应有的特性或状态来破坏系统信息完整性，目前主要通过访问控制技术保证信息完整性[22]。

5) 新鲜性。新鲜性主要是用来防止重放攻击，一般采用同步机制，如时间戳、同步序列（SQN，sequence number）等方式保证新鲜性[23]。

6) 不可抵赖性。不可抵赖性主要是防止消息发送方和接收方对自己发送或接收行为的否认，采用的技术手段一般是数字签名、签收机制等。

以上安全需求是保证移动通信网安全的基本需求，在每一代移动通信网标准制定之时都需要保证上述需求得到满足，否则会导致被攻击者利用的漏洞。这些安全需求也为移动通信安全技术发展指明了方向。随着社会的发展，人们会越来越关注移动通信网的安全问题，这些问题必须得到移动通信网研发人员的关注。针对这些安全需求，当前商用的移动通信系统还有很大的提升空间。

3　历代通信网的鉴权技术

纵观历代移动通信网鉴权技术，从鉴权方向上可以分为两大类：单向鉴权和双向鉴权。其中，单向鉴权是指网络对用户的鉴权，用户不对网络进行鉴权；双向鉴权是指用户和网络相互鉴权。本节对这两类鉴权技术分别介绍。

3.1　单向鉴权

单向鉴权主要在第二代移动通信系统中使用，2G 主要包括基于 GSM09.02 MAP 的泛欧数字移动通信系统（GSM, global system for mobile communications）和基于 IS-41 MAP 的北美数字移动通信系统，如码分多址（CDMA，code division multiple access），它们各成一派，形成了两大有代表性的用户鉴权技术体系[24]。

3.1.1　GSM 系统鉴权

在第一代模拟通信系统中，由于几乎没有安全机制保护，用户通话被窃听、号码被盗用、通信资源被窃取等安全问题层出不穷，严重损害了合法用户和运营商权益，加上模拟通信的服务能力限制，第二代移动通信技术应运而生。相比第一代模拟通信，采用数字通信的第二代通信系统增加了许多安全能力，这使 2G 成为当时最安全的移动通信系统，2G 系统所采取的保密措施主要有 4 种：防止空口信息被攻击者窃听的加解密技术；防止未授权用户非法接入的鉴权认证技术；防止攻击者窃取用户身份标识码和位置信息的临时移动用户身份更新技术；防止过期合法用户移动终端在网络中继续使用的设备认证技术[25]。鉴权认证技术就是防止未授权的用户接入 GSM 系统，其基本原理是在用户和网络之间运行鉴权和密钥协商协议，当移动终端访问拜访位置寄存器（VLR，visitor location register）时，网络对用户

的身份进行鉴别。

第二代移动通信网中最常见的鉴权发生在用户和基站之间，GSM 系统中鉴权规程在 GSM09.02 MAP 中定义。简要过程如下：当移动终端在拜访地期望连接网络时，终端便向拜访地网络发起鉴权请求，VLR 将该请求转发给归属地位置寄存器（HLR，home location register），归属地核心网收到请求后，基站首先产生一个随机数（RAND，random number），然后使用加密算法 A3 和 A8 将这个随机数和根密钥一起计算得出期望的鉴权响应号（SRES，signed response），同时基站把这个随机数发送给终端，上述过程在鉴权中心（AUC，authentication center）完成。在终端侧，用户设备根据收到的 RAND，并结合 IMSI 计算出鉴权响应号 SRES。随后终端将 SRES 通过空中信道发送给基站，基站将用户发送的鉴权响应号 SRES 和核心网计算得到的鉴权响应号进行比对。若二者一致，则鉴权成功，否则鉴权失败[26]。整个鉴权过程如图 1 所示。

3.1.2　CDMA 系统鉴权

CDMA 系统的鉴权流程在 IS-41 MAP 中被详细定义。当移动终端进入一个新的基站子系统（BSS，base station subsystem）时，它将收到新的 OMT（Overhead Message Train）基站系统广播消息，用户设备据此判断自己是否需要重新鉴权。此时，移动终端也会收到由无线基站控制器（BSC，base station controller）生成鉴权随机数 RAND，移动终端将收到的 RAND 值保存，在随后的鉴权验证值 AUTHx 生成时可以使用。CDMA 系统中用于移动台鉴权的密码分为两级；第一级为移动台的密钥 A_Key，第二级为共享加密数据（SSD，shared secret data）。密钥 A_Key 是高级密码，长度为 64 bit，由运营商分配，它和 IMSI 一同被写入移动终端永久性存储器中。同时，运营商核心网存储该用户的 IMSI 和对应的 A_Key。该密钥是永久性的，不在网络和空中信道上传播。SSD 是低级密码，长为 128 bit（分为 SSD_A 为 64 bit 和 SSD_B 为 64 bit），它由 A_Key 运算产生，存在于移动台、鉴权中心和拜访者位置寄存器[27]。在鉴权过程中，核心网使用 RAND 和 SSD_A 计算出期望的响应 AUTHx，倘若移动终端计算的 AUTHx（用 RAND 和 SSD_A 计算所得）和核心网计算的 AUTHx 相同，则鉴权成功，攻击者因没有正确有效的 SSD 值，无法计算得到核心网所期望的 AUTHx 值导致鉴权失败[28-30]。

3.2　双向鉴权

3.2.1　UMTS 系统鉴权

传统的 GSM 网络没有专门针对信令、语音和用户数据提供独立的完整性保护[31-33]，这是由

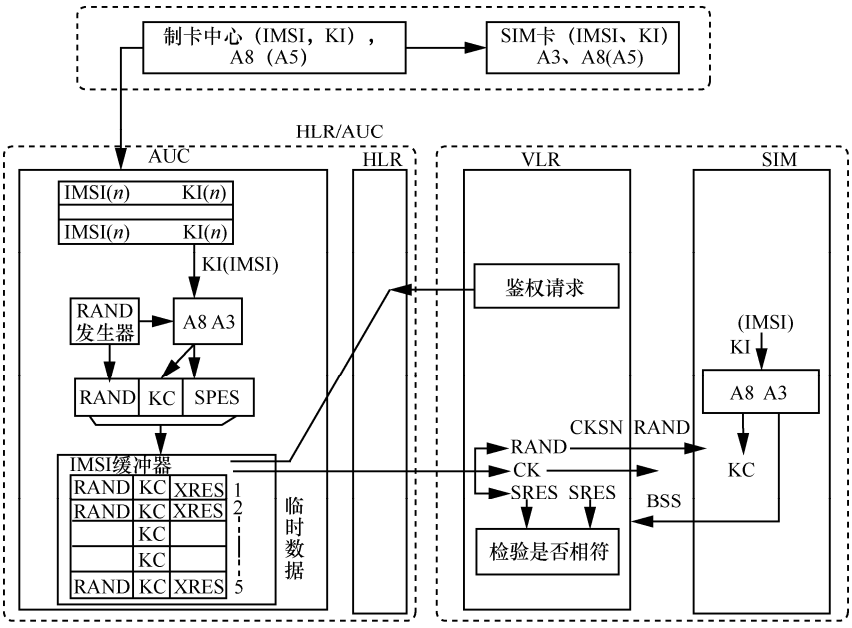

图 1　GSM 系统的鉴权过程

于在通信系统设计之初，人们重点考虑的是语音的传输，涉及的主要安全问题是空口信息传输时如何防止语音信息被窃听、用户信息被泄露，并未充分考虑对信息篡改或者伪造等问题的防护。因此对于信息可能被篡改的攻击，GSM 系统并未设计独立的完整性保护算法，而是通过在使用加密的方式同时实现对信息的完整性保护，即通过加密的方式，使攻击者无法获知明文，进而无法对密文进行修改。此外，GSM 系统用户极易被攻击者跟踪，而且攻击者只需要采取简单的措施就可以偷听用户的电话。2G 中的 VoIP 为运营商降低运营成本的同时，极大地增加了安全隐患，基于开放式标准的 VoIP 系统流量没有采取加密措施，攻击者可以轻易地偷听、拦截和伪造呼叫语音信息。如上所述，GSM 系统所采用的单向鉴权只有网络对终端的鉴权，没有终端对网络的鉴权，并且加密功能是否开启完全由网络侧决定。由于 GSM 协议的缺省版本并不采用加密技术，无法对基站进行甄别，最终造成了潜在的威胁。比较典型的有中间人攻击，一般过程如下：攻击者在用户终端和真基站之间安装假冒基站，从而形成自己的小区，一般攻击者基站的功率较大，移动终端自动地向功率较大的基站发送附着请求，这便暴露了自己的 IMSI。随后，攻击者侦听设备冒充目标终端向运营商真实网络侧发起注册请求，在这个过程中，把网络下发的 RAND 转给受害者移动终端，并把终端返回的 SRES 转给网络，这就完成了鉴权认证流程，完成鉴权后假基站截取终端和真基站之间的通信，而真基站和受害者终端都无法察觉[34]。此外，2G 通信系统中只有空口信息被加密，空口消息加密密钥长度只有 64 bit，目前这种长度的密钥已不安全[35]，核心网内部以及拜访地网络和归属地网络之间传输的消息仍是明文的，这也增加了网络安全风险。

3G 对 2G 安全性进行了改进，为了防止攻击者伪造网络，3G 通信系统增加了用户对网络的鉴权，这一特性是在鉴权和密钥协商协议中实现的，在此过程中也实现了加密算法协商和完整性密钥协商。通过实现算法协商，增加了系统的灵活性，使不同的运营商之间只要支持一种相同的 UEA/UIA 就可以跨网通信。3G 网络认证向量中的认证令牌（AUTN，authentication token）包含了一个序列号，该序列号可以使用户免受重传攻击，但可能会暴露用户的身份和位置信息，因此采用匿名密钥（AK，anonymity key）在 AUTN 中隐藏序列号。

在 3G 系统中，鉴权认证思想可以简单地概括为：SGSN/VLR 接收到来自移动台（MS，moving station）的响应 RES 后，将比较移动台 RES 与认证向量（AV，authentication vector）中的 XRES，若一致则鉴权成功，否则鉴权失败[36]。

具体来说，UMTS 系统中的鉴权过程如下。

1) 鉴权五元组生成：首先移动台拜访地网络发出接入请求，拜访地网络将该请求传送到归属地网络，归属地网络中的 HLR/AuC 生成鉴权向量，该向量由五元组（RAND，XRES，CK，IK，AUTN）构成。其中，RAND 是随机数，XRES 是期望的响应，CK 是机密性密钥，IK 是完整性密钥，AUTN 是鉴权令牌。

2) 归属地网络将鉴权向量发送到用户设备所在的拜访地网络。

3) 拜访地网络从收到的鉴权向量中选择一个，发送 RAND (i)、AUTN(i)到用户。

4) 用户侧再检查 AUTN (i)可否接受，随后计算消息认证码 XMAC，并与 AUTN 中的消息认证码（MAC，message authentication code) 比较，若不同则放弃认证过程。同时 MS 要核验 SQN 是否在有效的范围内，若不在则 MS 放弃认证过程，这实际上是用户终端对网络的鉴权过程。

5) 当以上验证步骤成功，终端产生响应 RES(i)送回拜访地网络 VLR/SGSN，拜访地网络比较 RES(i)和 XRES(i)，若一致则鉴权通过，否则鉴权失败。在鉴权成功后终端 USIM 卡同时 CK 和 IK，用于在空中接口加密和完整性保护。

完整的鉴权过程如图 2 所示。

3.2.2 LTE 系统鉴权

相比 3G，长期演进（LTE，long term evolution）简化了网络架构，采用 eNB 单层结

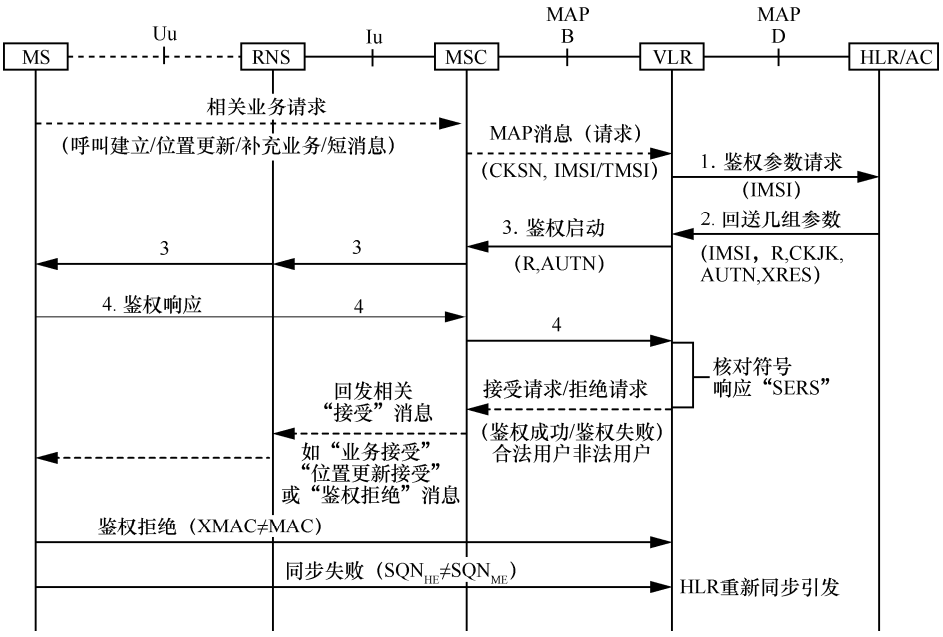

图 2　UMTS 系统的鉴权过程

构，实现了低复杂度和低时延的要求。虽然 3G 网络是在 2G 基础上的演进，解决了许多 2G 网络中存在的安全问题（如单向鉴权），但随着时间的推移，3G 网络暴露出了许多安全问题，具体有以下几类。

1) 3G 鉴权认证过程中虽然增加了终端对网络的认证，但仅对归属地网络 HLR 进行认证，并没有认证拜访地网络 VLR，利用这一漏洞攻击者就可以在空口截获合法的 IMSI 进行攻击。

2) 3G 网络没有对网络内部的通信链路进行保护，攻击者在 VLR 和 HLR 之间的通信链路上嗅探鉴权向量 **AV**，从而获得 CK 和 IK。

3) 3G AKA 也暴露出一些隐私问题，如攻击者通过重放预先截获某用户的认证令牌（AUTN），借助 3G AKA 对消息鉴权码（MAC，message authentication code）校验失败和同步失败的提示不同，判断该特定用户是否在当前小区内[37]。

总之，3G 系统的安全性有一个前提：整个网络内部是可信的。鉴于 3G 网络安全机制的漏洞，LTE 网络建立了分层安全机制。即 LTE 将安全在接入层（AS，access stratum）和非接入层（NAS，non-access stratum）信令之间分离，空口和核心网都有各自的密钥。第一层为 E-UTRAN 中的无线资源控制（RRC，radio resource control）层安全和用户层安全，第二层是演进分组核心网（EPC，evolved packet core）中的 NAS 信令安全，如图 3 所示[38]。

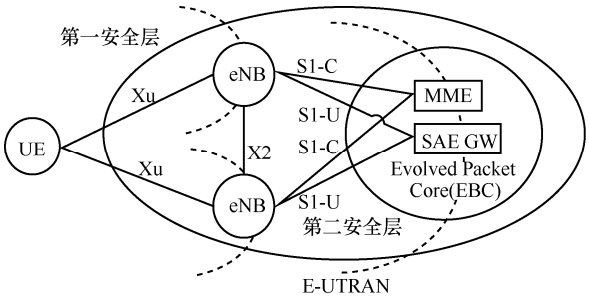

图 3　LTE 安全层次

鉴权数据分发过程阐述如下：MME 向归属地环境（HE，home environment）发送携带有 IMSI 的鉴权数据请求消息[39]，HE 利用 IMSI 找到与之对应的根密钥 K，并计算出鉴权向量。同 3G 网络不同，LTE 网络鉴权向量是四元组，即（RAND，AUTN，XRES，K_{ASME}）[40]。鉴权向量生成过程如图 4 所示，K、AMF、SQN 和 RAND 通过 f1[41]算法计算得出 MAC，K 和 RAND 通过 f2[41]算法计算得出 XRES，K_{ASME} 由 CK 和 IK 计算得到，IK、CK 的计算过程类似。

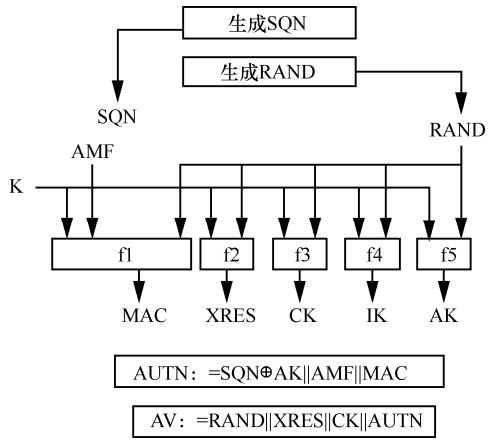

图 4　LTE 鉴权向量生成

MME 接收到鉴权向量后，将鉴权向量中的 RAND、AUTN 和 KSlasme 发送给 UE[42-43]，USIM 中用户鉴权参数生成过程如图 5 所示。UE 接收到鉴权请求消息后，通过 f5[41]和 f1 算法计算出 XMAC，并将计算结果与 AUTN 中的 MAC 进行比较，若二者一致则网络合法，否则网络非法。同时，UE 通过检验 SQN 是否在有效的范围内判断其是否合法，用以防范重放攻击。若上述两项验证均成功，则 UE 使用 K 和 RAND 通过 f2 算法计算出 RES，并将 RES 通过鉴权响应消息发送给 MME，MME 将接收到的 RES 与鉴权向量中的 XRES 进行比较，若一致则鉴权成功，否则鉴权失败。因此，4G 系统的鉴权也是双向鉴权的。

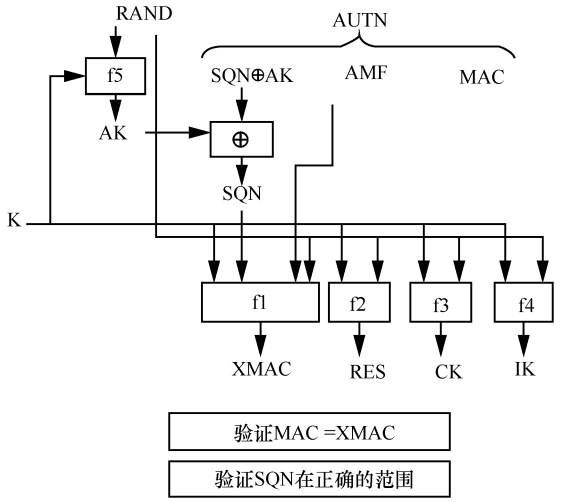

图 5　USIM 中用户鉴权处理

在上述鉴权过程完成后还要进行密钥协商，USIM 使用永久密钥 K 和随机数 RAND 分别通过 f3 和 f4[41]算法计算出 CK、IK，UE 利用 CK、IK 绑定服务网络标识并计算出 K_{ASME}，并将其与 KSlasme 对应起来存储。经过上述过程后，网络和 UE 之间完成了双向鉴权，并共享密钥 K_{ASME}，该密钥可以在随后用来计算 NAS 层密钥和 AS 层密钥。

4　5G 系统鉴权分析

4.1　上一代鉴权认证技术不足

虽然 LTE 系统的安全层次和密钥管理机制相比 3G 系统有了很大改进，但是仍存在 3 个方面的安全问题。

一是密钥安全体系仍然不够完善。LTE 系统用户鉴权和密钥协商机制采用分层的密钥体系，即根密钥 K 是永久性根密钥，机密性密钥 CK 和完整性保护密钥 IK 是鉴权中心 AuC 和 USIM 卡在 AKA 认证过程中根据 K 和 RAND 协商的一对密钥，而终端侧和核心网侧的所有中间密钥（KeNB，KUP，KASME，KNAS）均是通过 CK 和 IK 推演得到的，由此可见，根密钥 K 是 LTE/SAE 移动通信网络整个安全体系的根基，倘若攻击者获得了 K 这个根密钥，则整个 LTE 网络对攻击者而言就是透明的。攻击者可以采用主动攻击手段攻击 eNB，也可以采用被动攻击手段在空中信道窃听核心网发送的鉴权向量和用户终端发送的响应 RES。而根密钥 K 是保持不变的，攻击者通过学习大量的鉴权参数样本就可以进行猜测攻击[44]。

二是存在密码体制的局限性，LTE 网络采用对称密码体制。虽然对称密码体制具有安全性能高、算法处理速度快的优点，但在密钥协商完成之前，网络和 UE 必须以明文传递消息，这直接导致了鉴权认证之前的信令不能被有效保护，故在 2G、3G、4G 通信系统中一直存在 IMSI catcher 问题。这是对称密码体制的天然缺陷所导致的、而非对称密码体制能够有效解决的一问题。

IMSI catcher 问题、就是攻击者利用各种无线电工具进行鉴权信令截获和重传，在此过程中获取合法用户真实身份 IMSI。为了防止用户位置被跟踪，LTE 系统平时传递数据都是使用临时移动用户身份标识（TMSI，temporary mobile subscriber identity），移动终端只有在 2 种特殊的场景下发送

自己的 IMSI。第一种场景是被动侦听。当手机正常开机接入网络时，先从 USIM 中读取之前运营商分配的临时身份信息，将携带该信息的信令发送给基站，请求接入运营商网络。基站收到该消息后转发给核心网的移动性管理实体（MME，mobility management entity），若 MME 中可以查询到 GUTI/TMSI 对应的真实身份，则允许手机接入。若 MME 查询不到，则核心网需要重新对手机发起真实身份核验的请求“Identity Request”消息，即要求手机提供真实身份 IMSI。这种情形常常发生在手机首次入网或手机移动到其他 MME 覆盖范围后，MME 无法从核心网数据库中查询到手机的 TMSI，故需要手机上报自己的真实身份，此时攻击者只需在空口采取被动监听就可以捕获手机的 IMSI。第二种场景是主动获取。由于手机主动选择信号强度最强的基站进行附着操作，伪基站通过发射比真实基站信号强度高的无线信号，使受害者手机主动附着在伪基站上，之后强行给连接过来的手机发送身份验证请求消息“Identity Request”，手机便将真实身份 IMSI 上报给伪基站。此时主动攻击者只需要打开伪基站，不停地发送“Identity Request”消息就可以不断获取周围小区内手机的真实身份 IMSI。比较有名的一款 IMSI Catcher 工具叫黄貂鱼（Stingray），Stingray 是一款同时具有被动监听（如监听、数据分析）和主动攻击（如构造伪基站）的 IMSI Catcher。该设备轻巧便携，还可以测绘基站的分布情况，自行进行数据分析，监听通信内容，追踪目标手机位置，进行 DDoS 攻击等[45-46]。

三是 eNB 安全问题。3GPP 认为若 eNB 被部署在不安全环境中，eNB 面临的一个很大的安全问题是攻击者直接非法占领控制该 eNB，由于目标 eNB 的密钥 K_{eNB} 可以经源 eNB 上的密钥 K_{eNB} 推演得到，倘若攻击者控制了源 eNB，就可以推演得到目标 eNB 的密钥 K_{eNB}，导致威胁逐步扩散。那么当用户终端跨小区切换时终端密钥不具备用户设备切换时，接入层密钥（K_{eNB}）更新不具备后向安全性[44]。

4.2 5G 系统鉴权

2018 年 6 月，在 3GPP 第 80 次全会上 5G 独立组网（SA，stand alone）标准冻结，这是 5G 标准的第一个完整版本，在此前的 2017 年 12 月 3GPP 第 78 次全会上冻结了 5G 非独立组网（NSA，non-stand alone）的新空口（NR，new radio）标准。这些标准中对 5G 鉴权方案进行了明确。其中，针对 4G 网络鉴权中存在的安全问题，5G 鉴权方案专门做了修正，最典型的就是使用公私钥加密体制防止 IMSI 被捕获。手机的真实身份在 5G 中称为 SUPI（subscription permanent identifier）（类似于 IMSI），通过公钥加密后的密文称为 SUCI（subscription concealed identifier），SUCI 传送给基站后，基站直接上传至核心网，大致的流程如图 6 所示[21,47]。

5G 系统有 2 种鉴权认证协议，分别为 5G AKA 和 EAP-AKA'。EAP-AKA'与 5G AKA 非常相似：它们依赖于相同的安全机制，如 K 作为共享秘密的挑战响应，SQN 用于重放攻击保护，并使用类似的加密消息。主要区别是一些具体流程和一些关键的派生函数略有改变，这里主要介绍采用 5G AKA 协议进行鉴权认证。当服务网络（SN，serving network）触发了与用户的认证，用户终端就会发送 SUPI 的随机加密：SUCI =⟨aenc（⟨SUPI，Rs⟩，pkHN），idHN⟩，其中，aenc（·）表示非对称加密，Rs 是随机数，而 idHN 唯一地标识为归属地网络（HN，home network）。标识符 idHN 使 SN 能够从合适的 HN 请求认证资料。在接收到 SUCI 以及 SN 的身份（称为 SNname）时，HN 可以检索 SUPI、用户的身份，并选择认证方法。请注意，SUPI 还包含 idHN，因此标识用户及其 HN。如前所述，密钥 K 用作长期共享密钥，SQN 为用户提供重放保护。虽然 SQN 应该在用户和 HN 之间同步，但可能发生不同步（如由于消息丢失），因此，使用 SQN_{UE}（分别为 SQN_{HN}）指代存储在 UE（分别为 HN）中的 SQN 值。5G-AKA 协议包括 2 个主要阶段：质询−响应和可选的重新同步流程（在 SQN 不同步的情况下更新 HN 侧的 SQN）。

第一阶段是质询−响应。在收到鉴权认证请求后，HN 从以下参数构建认证质询：随机数 R（即 challenge）、AUTN（证明挑战的新鲜度和真实性）、HXRES *（SN 期望的对 challenge 的响应）、

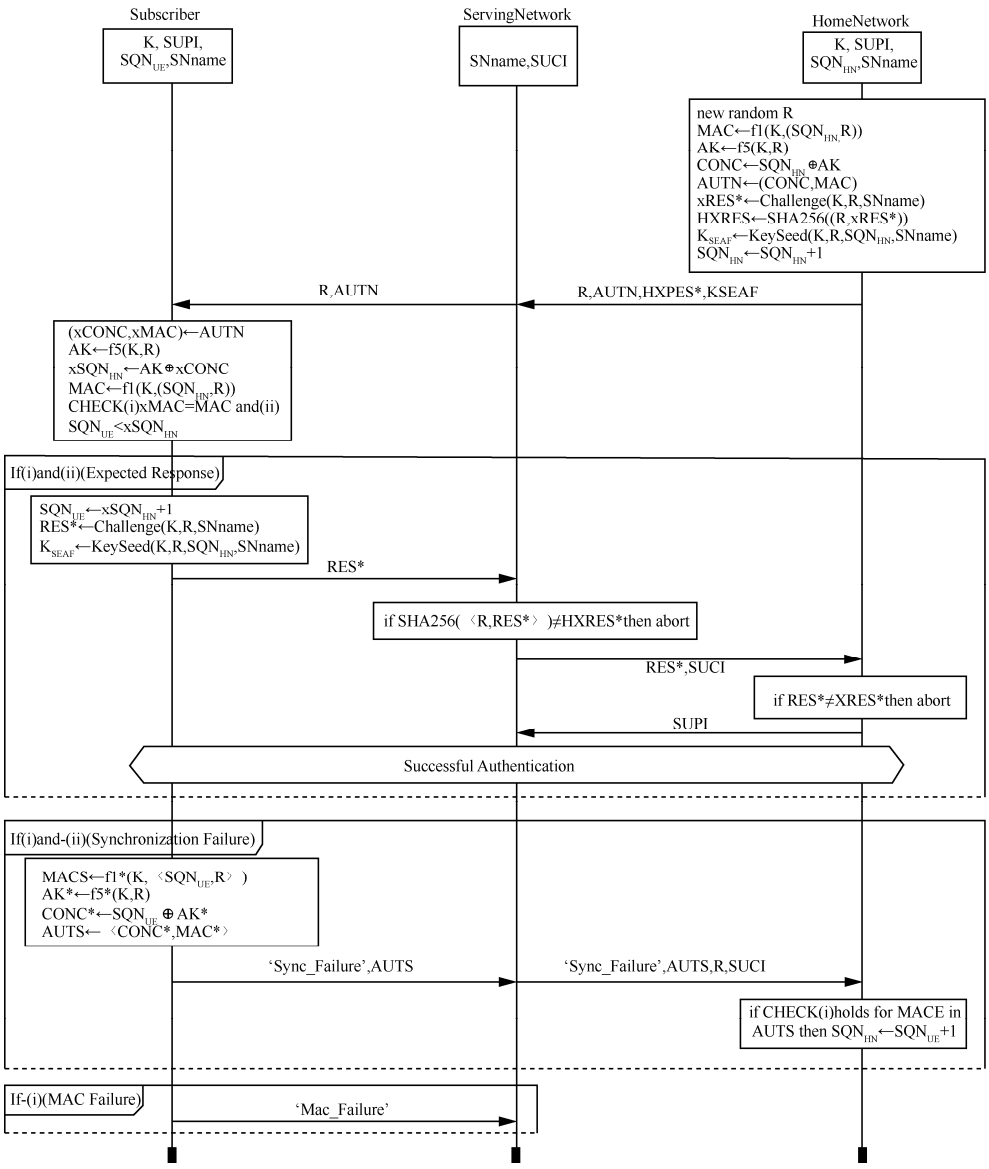

图 6　5G AKA 鉴权过程

K_{SEAF}（用以用户和 SN 安全信道的建立）。函数 f1～f5 用于计算身份验证参数，是单向密钥加密函数，这些函数彼此完全无关，⊕表示异或。Challenge（·）和 KeySeed（·）是复杂的密钥衍生函数（KDF，key derivation function），AUTN 包含 R 的串联消息认证码（MAC），其具有为该用户存储的相应序列号 SQN_{HN}，SQN_{HN} 的值通过递增计数器生成。序列号 SQN_{HN} 的作用是允许用户验证认证请求的新鲜度以防止重放攻击，并且 MAC 证明了 challenge 的真实性。HN 不会将质询的完整响应 RES *发送给 SN，而只发送其中的散列值，这是出于保护用户信息的目的。因为 HN 对 SN 并不是完全信任的，如果 SN 被攻击者控制，则 HN 发送完整的 RES * 会泄露用户信息。

SN 存储 K_{SEAF} 和 challenge 的预期响应，然后将 challenge 转发给用户。收到挑战后，用户首先检查其真实性和新鲜度。为此，用户从 AUTN 中提取 $xSQN_{HN}$ 和 MAC 并检查。

1) MAC 是否是相对于 K 的正确 MAC 值，如果不是，则回复 MAC 校验失败消息 'Mac_failure'。

2) 认证请求是否新鲜，即 SQN_{UE} <$xSQN_{HN}$，如果不是，则回复同步失败<'Sync_failure'，

AUTS>（AUTS 在下面的重新同步过程中解释）。

如果所有检查都通过，则用户计算密钥 K_{SEAF}，用于保护后续消息，它还计算认证响应 RES*并将其发送到 SN。SN 检查该响应是否符合预期，并转发给验证它的 HN。如果此验证成功，则 HN 向 SN 确认认证成功并将 SUPI 发送到 SN，并且使用密钥 K_{SEAF} 保护 SN 和用户之间的后续通信。

在同步失败的情况下（情况 2)），用户回复<'Sync_failure', AUTS>，还要发起重新同步流程。AUTS 消息使 HN 能够通过用户 SQN_{UE} 的序列号替换它自己的 SQN_{HN} 来与用户重新同步，但 SQN_{UE} 不会以明文形式传输，以避免被窃听。因此，该规范要求隐藏 SQN，即它与一个值保持私有的异或：AK * = f5 *（K，R）。形式上，隐藏值是 CONC * =SQN_{UE}⊕AK*，它允许 HN 通过计算 AK *来提取 SQN_{UE}。请注意，f5 *和 f1 *是独立的单向密钥加密函数，与函数 f1~f5 完全无关。最后，AUTS =⟨CONC*，MAC *⟩，其中，MAC * = f1 *（K，⟨SQNUE，R⟩），允许 HN 将该消息认证为来自预期用户。

目前，3GPP 标准中已经明确了以下内容：手机端用来加密 SUPI 的公钥存放在 UICC 的 USIM 中；SUCI 的解密算法（SIDF）只被执行一次，放置在核心网的 UDM 中；当手机临时身份 GUTI 无法识别时，由接入和移动性管理网元（AMF，access and mobility management function）向手机发起 Identity Request 请求；若手机在注册紧急服务时收到 Identity Request 发送 Null-Scheme 的 SUCI，即不加密的 SUPI；由 AMF 负责配置发送手机的 5G-GUTI；SUCI 的生成算法可以采用椭圆曲线集成加密方案（ECIES，elliptic curve integrate encrypt scheme）[48]，运营商也可以根据自己需求自拟方案，甚至可以采用 Null-Scheme。

5G 鉴权方案中，通过公私钥方案将 SUPI 加密为 SUCI 是一个亮点，它有效地避免了用户真实身份 SUPI 在空口传播。在图 7 和图 8 中可以看到两对密钥对，一对是终端侧产生的公钥 Eph. public key 和私钥 Eph. private key，另外一对是运营商网络产生的，终端侧有网络侧产生的公钥固定存放在 USIM 中，网络侧存有用户终端产生的公钥（由终端发送给网络），这两对密钥均采用椭圆曲线加密（ECC）算法生成。图 8 给出 UE 侧将 SUPI 加密为 SUCI 的方案，首先终端生成的私钥与网络提供的公钥结合，派生出一对用来加密的原始密钥 Eph.shared key，随后据此派生出加密的主密钥，取高有效位对 SUPI 进行对称加密得到 SUCI；而低有效位对所有的有用信息进行完整性保护，如包含终端参数等。所以最后终端发出的消息包括终端生成的公钥、SUCI 和终端参数等系列信息。

图 8 为网络侧对终端身份进行验证的方案。网络侧采用私钥（private key of HN）与终端所发

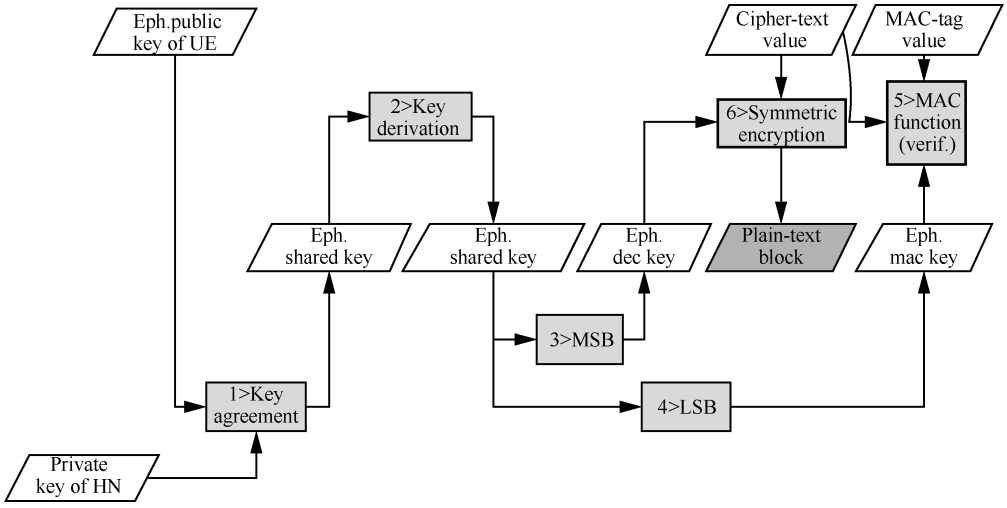

图 7 网络侧对终端的验证方案

送的公钥（Eph.public key of UE）组合成密钥 Eph.shared key，随后据此派生出主密钥 master key。但这里与终端加密 SUPI 稍有不同，网络侧先利用密钥的低有效位进行消息完整性校验，若消息经过攻击者篡改，则该步骤的验证无法通过。只有当验证通过后，才会进一步将信令消息转发至统一数据管理（UDM，unified data management）网元，UDM 再调用 SIDF（Subscription identifier de-concealing function）网元将 SUCI 解密得到 SUPI。接下来，核心网根据手机的鉴权方式逐一提取对应的鉴权密钥与鉴权结果，直至最后将结果反馈给手机，手机端 USIM 校验网络侧所发送鉴权结果的真伪。

该方案可以顺利通过验证并解密得到 SUPI 的关键也是利用椭圆加密算法的特性：若终端与网络侧均采用同一条曲线，即椭圆曲线的参数一致（Curve25519[49] 或 secp256r1[50]）。而密钥之间的乘法是椭圆曲线上的标量乘法，终端私钥·网络公钥=网络私钥·终端公钥，这样便利用两对非对称密钥组合成一对对称密钥。

4.3　5G 系统鉴权安全性分析

虽然符合 3GPP 标准的 5G 商用网络尚未部署，但是已经有研究人员针对现有 5G 标准进行安全性研究[51-53]。Basin 等[51]使用形式验证工具分析 5G AKA 算法，并证明该协议未能满足明确要求的若干安全目标。该研究还表明，5G 协议缺乏其他关键的安全属性。这些发现给 5G 带来了压力，与 LTE 的情况不同，一旦协议被定义、实施和全球部署，大多数安全研究和由此产生的协议缺陷都被确定，安全研究人员正在快速推进 5G 研究，尽量使标准组织在编写规范时识别相应漏洞。

只有全面的全球运营商都严格按照 3GPP 标准部署 5G 网络，5G 安全基础架构才具有其期望的安全性。这要求全球所有运营商无一例外地在自己所管理的 SIM 卡中的其他国家运营商的公钥或证书。然而，纵观历代移动通信网部署情况，出于成本等种种原因，并非标准规定的所有安全措施都被运营商严格落实。这一现象在 5G 网络中有可能继续出现，一些运营商不会选择实施所有 5G 安全功能，另一方面，5G 公钥基础设施（PKI，public key infrastructure）实施的大多数实际细节明确不属于 3GPP 的范围[54]。此外，一些国家或许还将禁止其他国家或运营商的证书，因此，全球采用和严格实施 5G 安全功能的可能性极小。由于 SIM 卡不会为所有国家和地区的移动运营商提供公钥或证书，因此 UE /运营商有 2 种选择：①明确阻止未能提供公钥或证书的运营商接入网络，并处理由此产生的公共关系和媒体报道后果；②允许这种极端情况的出现，即让这些运营商接入全球网络，虽然这会破坏全球 5G 网络安全秩序。5G 安全规范最终采用选项②，明确规定如果没有为用户的 USIM 提供服务网络，则用户身份将不受保护[21]，这意味着 5G 中明文传输 IMSI/SUPI 的现象仍然存在。

目前，3GPP 还未明确的问题有：GUTI 更新

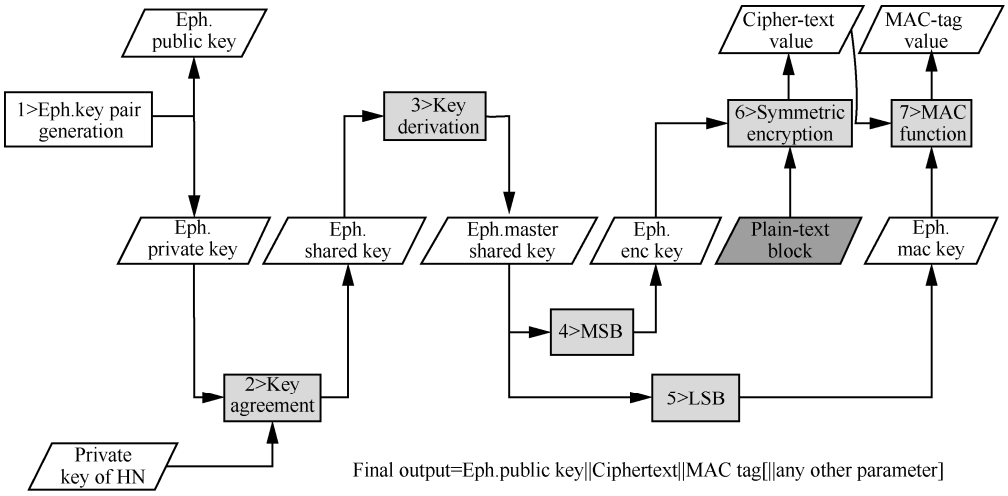

图 8　终端侧 SUCI 生成方案

的频率未做硬性规定，这由运营商自行决定。需要注意的是，GUTI 虽然是临时身份证，但如果长时间保持不变，则可能被攻击者利用从而实现在一段时间内的位置跟踪。另一个是终端对网络上报 SUCI 的频率未做硬性规定。当手机在收到网络侧发送的身份认证请求时，需要回复 SUCI。手机要保证每次发送的 SUCI 都是新鲜的、随机的。但伪基站仍可以不断要求手机发送 SUCI，这会导致手机电力消耗或者发起 DoS 攻击等。

5 统一认证技术

在以往的通信系统中，主要满足的是人与人之间的通信，而 5G 网络需要满足人与物以及物与物之间的通信，因此 5G 需要支持多种网络的接入，如无线局域网络（WLAN，wireless local area networks）、LTE、固定网络、5G NR、物联网（IoT，Internet of things）、卫星接入、车联网等，而不同的网络所使用的接入技术不同，因此有不同的安全需求和接入认证机制。再者，由于各种智能穿戴设备的兴起，一个用户可能携带多个终端，而一个终端也可能同时支持多种接入方式，有些场景可能需要同一个终端在不同接入方式之间进行切换，或者用户在使用不同终端进行同一个业务时，要求能进行快速认证以保持业务的延续性从而获得流畅的用户体验。因此，5G 网络需要构建一个统一的认证框架来融合不同的接入认证方式，此外还要针对不同的接入认证方式优化鉴权认证协议，如上下文的安全传输、密钥更新管理等，以提高终端在异构网络间进行切换时的安全认证效率，同时还能确保同一业务在更换终端或更换接入方式时能够获得连续的业务安全保护[55]。

多种设备接入必然导致不同类型设备计算能力的差异，即便同一类型设备计算能力也可能差异较大。如有些物联网设备要求轻量节能，需要一年或好几年更换一次，而有些物联网设备则不用太在意能耗问题，相比于物联网设备，手机的计算能力在不断增强，已经赶上或超越某些笔记本电脑的计算能力。在 5G 应用场景中，计算能力强的设备可能配有 SIM/USIM 卡，并具有一定存储能力，有些终端设备没有 SIM/USIM 卡，其身份标识可能是 IP 地址、MAC（介质访问控制）地址、数字证书等；而有些能力低的终端设备，甚至没有特定的硬件来安全存储身份标识及认证凭证，因此，5G 网络需要构建一个统一的身份管理系统，使得其能够支持不同的认证方式、认证凭证和身份标识。

可扩展认证协议（EAP，extensible authentication protocol）认证框架在 RFC 3748 中定义[56]，是能满足 5G 统一认证需求的备选方案之一，EAP 认证框架是一种支持多种认证方法的三方认证框架，能封装多种认证协议，如鉴权和密钥协商（EAP-AKA）、预共享密钥（EAP-PSK）、传输层安全（EAP-TLS）等。在 3GPP 目前所定义的 5G 网络架构中，认证服务器功能（AUSF，authentication server function）和认证凭证库和处理功能（ARPF，repository and processing function）网元可完成传统 EAP 框架下的认证服务器功能，接入管理功能 AMF 网元可完成接入控制和移动性管理功能，5G 统一认证框架如图 9 所示。

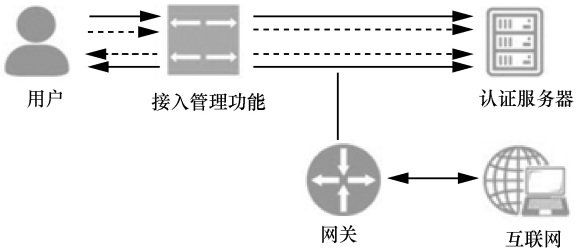

图 9 统一认证框架

3GPP 在 R15 阶段的文档 TR 33.899[54]中阐述了 EAP 框架用作 5G 统一认证框架备选方案，框架适用于任何类型的用户以任何一种 3GPP 接入技术（如 2G/3G/4G）和非 3GPP 接入技术（如 WiMAX，Wi-Fi）进行接入鉴权认证。目前，EAP 支持的认证方法有 EAP-TLS、EAP-SIM、EAP-MD5 等[57]。在 5G 统一认证框架中，各种接入方式均可在 EAP 框架下接入 5G 核心网：用户通过 WLAN 接入时可使用 EAP-AKA′协议，有线接入时可采用 IEEE 802.1x 认证，5G NR 接入时可使用 5G-AKA 认证。虽然接入方式不同，但不同的接入网在逻辑功能上使用统一的 AMF 和 AUSF/ARPF 提供认证服务，这样用户在不同接

入网间进行无缝切换成为可能。

5G 网络的安全架构与以往的移动网络的安全架构区别很大，引入统一认证框架不仅能降低运营商的投资和运营成本，也为将来 5G 网络提供新业务时对用户的认证打下坚实的基础，极大地增加了 5G 的可扩展性。

6　历代鉴权技术比较

本节针对上文提到的鉴权机制进行总结，并对其优缺点进行对比分析，如表 1 所示。表 1 中没有加入统一认证机制，因为统一认证机制是一个融合的鉴权技术，至今还没有一种明确合适的方案。

7　结束语

针对第 5 代移动通信，3GPP 定义了 3 个标准版本（R14-R16）完成标准化工作，并于 2017 年底发布了第一个 5G 非独立组网的标准版本（5G NR NSA），能够支持部分运营商的组网需求，继而，3GPP 又于 2018 年 6 月发布了 5G 独立组网的标准版本（5G NR SA），进一步支持更多运营商的组网需求。面向 R16，3GPP 进行了更多技术的增强，使 5G 更好地满足 ITU 所定义的三大场景的要求。

5G 鉴权认证机制已经在 R15 版本中明确，但统一认证机制还有待在 R16 版本中继续明确。通过公私钥加密的方式，5G 杜绝了空口中 IMSI 泄露的问题，关闭了攻击者侵入核心网的第一道关口，大大提高了整个 5G 网络的安全性。尽管标准很完善，运营商在实际部署 5G 网络时可能为了在成本与收益之间取得平衡，或者说为了满足 5G 低时延特性，而不部署或者不完全部署 3GPP 标准中所规定的机制。另外，统一认证机制还有待完善，由于要接入各种类型的设备，其安全性直接影响整个 5G 网络的安全性。未来的网络鉴权机制应该朝着加密和认证算法轻量化、高效化、安全化的方向发展，以满足超低时延、用户隐私保护、网络安全的需求。此外，由于鉴权机制中涉及众多密码算法，而密码算法对保证安全通信至关重要，虽然 5G 所采用的密码算法（如 SNOW、ZUC、AES 等）目前均不存在安全性问题，但在后 5G 或者 5G 技术的演进过程中，研究人员应注意量子计算技术的发展，考虑密码算法的量子安全性，从而保证移动通信网鉴权认证机制的安全。

参考文献：

[1] SHAIK A , BORGAONKAR R , ASOKAN N , et al. Practical attacks against privacy and availability in 4G/LTE mobile communication systems[C]//Symposium on Network and Distributed Systems Security (NDSS) .2016.

[2] RUPPRECHTD, KOHLS K, HOLZ T, et al. Breaking LTE on layer two[C]//Symposium on Network and Distributed Systems Security (NDSS) .2018.

[3] 李涛. 网络安全概论[M]. 北京: 电子工业出版社, 2004.
LI T. Introduction to network security[M]. Beijing: Publishing House of Electronics Industry, 2004.

[4] 金东勋. GSM 网络安全协议漏洞研究[D]. 北京: 北京邮电大学, 2015.
JIN D X. Research on GSM network security protocol vulnerabilities[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[5] FOX D. IMSI-catcher[J]. Datenschutz und Datensicherheit (DuD), 1997, 21:539-539.

[6] STROBEL D. IMSI catcher[J]. Seminar Work, Ruhr-Universitat Bochum, 2007.

表 1　　移动通信网络鉴权技术对比

网络	元组	鉴权方向	优缺点
GSM	（SRES(*i*)，RAND，Kc(*i*)）	单向	具备一定的安全机制，三元组使用后会被破坏，不会重用，使用了 A3、A8 等算法加密，操作简单。单向鉴权，kc 只有 64 bit，存在明文发送 IMSI 情况
CDMA	（MIN，ESN，A-KEY，SSD-A，SSD-B）	单向	主密钥 A-KEY 不直接用于认证，2 个 SSD 共 128 bit。单向鉴权，操作复杂，存在明文发送 IMSI 情况
UMTS	（RAND，XRES，CK，IK，AUTN）	双向	提供接入链路的信令数据完整性保护，密钥长度为 64/128 bit，安全机制可拓展，双向鉴权避免伪基站，鉴权向量不可重用。存在明文发送 IMSI 情况
LTE	（RAND，AUTN，XRES，Kasme）	双向	分级密钥增强安全性，密钥长度 128 bit，双向鉴权避免伪基站。存在明文发送 IMSI 情况
5G	（RAND、AUTN、XRES*、K_{AUSF}）	双向	部分密钥长度为 128/256 bit，采用公私钥的方式加密 SUPI 不会明文发送 SUPI。加密算法复杂，增加 UE 功耗，可能会增大时延

[7] ARAPINIS M, MANCINI L, RITTER E, et al. New privacy issues in mobile telephony: fix and verification[C]//ACM Conference on Computer and Communications Security. 2012: 205-216.

[8] HUSSAIN S R, CHOWDHURY O, MEHNAZ S, et al. LTE Inspector: a systematic approach for adversarial testing of 4G LTE[C]// Symposium on Network and Distributed Systems Security (NDSS). 2018: 18-21.

[9] DAVID B, JANNIK D, LUCCA H, et al. A formal analysis of 5G authentication[C]//ACM Conference on Computer and Communications Security (CCS). 2018.

[10] 罗明星, 杨义先, 王励成, 等. 抗窃听的安全网络编码[J]. 中国科学: 信息科学, 2010, 40(2):371-380.
LUO M X, YANG Y X, WANG L C, et al. Secure network coding for anti-eavesdropping[J]. Science in China, 2010, 40(2): 371-380.

[11] 黄开枝, 王兵, 许晓明, 等. 基于安全保护域的增强型多点协作传输机制[J]. 电子与信息学报, 2018, 40(1):108-115.
HUANG K Z, WANG B, XU X M, et al. Enhanced multi-point cooperative transmission mechanism based on security protection domain[J]. Journal of Electronics & Information Technology, 2018, 40(1): 108-115.

[12] 邓晓明. 移动无线传感器网络复制节点攻击检测协议的研究[D]. 合肥: 中国科学技术大学, 2011.
DENG X M. Research on attack detection protocol of mobile wireless sensor network replication node[D]. Hefei: University of Science and Technology of China, 2011.

[13] 苏洪斌. 新技术下的移动通信网络安全[J]. 信息安全与通信保密, 2006(10):103-105.
SU H B. Mobile Communication network security under new technology[J]. Information Security & Communication Security, 2006(10): 103-105.

[14] 魏国珩, 秦艳琳, 张焕国. 基于 ECC 的轻量级射频识别安全认证协议[J]. 华中科技大学学报(自然科学版), 2018(1):49-52.
WEI G Z, QIN Y L ZHANG H G. Lightweight radio frequency identification security authentication protocol based on ECC[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2018(1): 49-52.

[15] 尚青为. 面向移动通信安全的伪基站识别机制研究[D]. 北京: 北京邮电大学, 2015.
SHANG Q W. Research on pseudo base station identification mechanism for mobile communication security[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[16] 谢刚. 下一代移动通信系统中混合自动重传机制的研究[D]. 北京: 北京邮电大学, 2007.
XIE G. Research on hybrid automatic retransmission mechanism in next generation mobile communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2007.

[17] 洼田光宏. 移动通信系统和重传控制方法: CN, CN 100547959 C[P]. 2009.
WA T G H. Mobile communication system and retransmission control method: CN, CN 100547959 C[P]. 2009.

[18] 严振亚. 下一代移动通信系统中的混合自动重传请求技术研究[D]. 北京: 北京邮电大学, 2007.
YAN Z Y. Research on hybrid automatic repeat request technology in next generation mobile communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2007.

[19] 李锐光, 黄文廷, 王永建. GPRS 网络中恶意代码监测技术研究[J]. 计算机研究与发展, 2012(s2):64-68.
LI R G, HUANG W T, WANG Y J. Research on malicious code monitoring technology in GPRS network[J]. Journal of Computer Research and Development, 2012(s2): 64-68.

[20] 程璟睿, 魏来, 周智. 中国移动恶意代码检测与治理方案[J]. 电信工程技术与标准化, 2013(2):61-65.
CHENG Y R, WEI L, ZHOU Z. China mobile malicious code detection and governance scheme[J]. Telecommunications Engineering Technology and Standardization, 2013(2): 61-65.

[21] 3GPP. Security architecture and procedures for 5G system (Release 15)[S]. 3GPP TS 33.501, 2018.

[22] 肖宁. WCDMA 系统接入安全实现机制的研究[J]. 重庆邮电大学学报(自然科学版), 2004, 16(3):43-46.
XIAO N. Research on access security implementation mechanism of WCDMA system[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2004, 16(3): 43-46.

[23] 杨先磊. 无线应用中身份认证技术的研究[D]. 北京: 北京邮电大学, 2007.
YANG X L. Research on identity authentication technology in wireless applications[D]. Beijing: Beijing University of Posts and Telecommunications, 2007.

[24] 王雅宁. 数字集群通信系统加密机制的研究[D]. 哈尔滨: 哈尔滨工业大学, 2006.
WANG Y N. Research on encryption mechanism of digital trunking communication system[D]. Harbin: Harbin Institute of Technology, 2006.

[25] 牛静媛. 移动通信系统安全性分析[D]. 北京: 北京邮电大学, 2008.
NIU J Y. Security analysis of mobile communication system[D]. Beijing: Beijing University of Posts and Telecommunications, 2008.

[26] 张磊. GSM/UMTS 混合网络安全若干关键技术研究[D]. 北京: 北京邮电大学, 2011.
ZHANG L. Research on several key technologies of GSM/UMTS hybrid network security[D]. Beijing: Beijing University of Posts and Telecommunications, 2011.

[27] 刘彩霞, 俞定玖, 邬江兴. 3G 中 A-Key 的产生和分配机制[J]. 计算机工程与科学, 2002, 24(5):25-27.
LIU C X, YU D X, WU J X. Generation and distribution mechanism of a-key in 3G[J]. Computer Engineering and Science, 2002, 24(5): 25-27.

[28] 800MHz CDMA 数字蜂窝移动通信网移动应用部分技术要求[S]. YD/T1202-2002, 2004.
800MHz CDMA digital cellular mobile communication network mobile application part technical requirements[S]. YD/T1202-2002, 2004.

[29] 陶启茜, 马金兰. CDMA 用户信息加密关键技术研究与实现方案探讨[J]. 电信科学, 2013(s2):38-42.
TAO Q Q, MA J L. Research and implementation of key technologies for CDMA user information encryption[J]. Telecommunications Science, 2013(s2): 38-42.

[30] 樊自甫, 杨俊蓉, 万晓榆. TD-SCDMA 与 GSM 互操作中基于鉴权原因的切换失败问题分析及解决[J]. 电信科学, 2010, 26(4):52-58.
FAN Z F, YANG J R, WAN X Y. Analysis and solution of switching failure problem based on authentication reason in TD-SCDMA and GSM interoperation[J]. Telecommunications Science, 2010, 26(4): 52-58.

[31] 3GPP. Security related network functions[S]. 3GPP TS 43.020, 2000.

[32] 3GPP. Security architecture (release 6)[S]. 3GPP TS 33. 102, 2001.

[33] 3GPP. Security objectives and Principles[S]. 3GPP TS 33. 120,

2001.
[34] 付航. GSM 网络安全问题分析及 3G 可信网络架构探讨[J]. 电信技术, 2009, 1(7):76-77.
FU H. Analysis of GSM network security issues and 3G trusted network architecture[J]. Telecommunications Technology, 2009, 1(7): 76-77.
[35] 张方舟, 叶润国, 冯彦君, 等. 3G 接入技术中认证鉴权的安全性研究[J]. 微电子学与计算机, 2004, 21(9):33-37.
ZHANG F Z, YE R G, FENG Y J, et al. Security research of authentication and authentication in 3G access technology[J]. Microelectronics & Computer, 2004, 21(9): 33-37.
[36] 冒海霞, 陈天洲, 戴鸿君. 高强度的移动通信安全中间件架构[J]. 计算机应用研究, 2006, 23(8):91-94.
MAO H X, CHEN T Z, DAI H J. High-strength mobile communication security middleware architecture[J]. Journal of Computer Applications, 2006, 23(8):91-94.
[37] ARAPINIS M, MANCINI L, RITTER E, et al. New privacy issues in mobile telephony:fix and verification[C]//ACM Conference on Computer and Communications Security. 2012:205-216.
[38] 曹俊华, 李小文. LTE/SAE 安全体系的研究及其在终端的实现[J]. 电信科学, 2010, 26(7):50-54.
CAO J H, LI X W. Research on LTE/SAE security system and its implementation in terminal[J]. Telecommunications Science, 2010, 26(7): 50-54.
[39] 3GPP. 3GPP System architecture evolution (SAE); security architecture[S]. 3GPP TS 33.401, 2011.
[40] 3GPP. 3G security; security architecture[S]. 3GPP TS33.102, 2014.
[41] 3GPP. 3G Security; document2: algorithm specification[S]. 3GPP TS 35.206, 2012.
[42] 3GPP. Non-access-stratum (NAS) protocol for evolved packet system (EPS); stage 3[S]. 3GPP TS 24.301, 2011.
[43] 3GPP. evolved universal terrestrial radio access (E-UTRA); Radio resource control (RRC) protocol specification[S]. 3GPP TS 36.331, 2011.
[44] CAO J, LI H, MA M, et al. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. Computer Networks, 2012, 56(8):2119-2131.
[45] DABROWSKI A. The messenger shoots back: network operator based IMSI catcher detection[C]//International Symposium on Research in Attacks, Intrusions, and Defenses. 2016.
[46] 陈飞, 毕小红, 王晶晶, 等. DDoS 攻击防御技术发展综述[J]. 网络与信息安全学报, 2017, 3(10):16-24.
CHEN F, BI X H, WANG J J, et al. Overview of DDoS attack defense technology development[J]. Journal of Network and Information Security, 2017, 3(10): 16-24.
[47] 3GPP. System architecture for the 5G System[S]. Stage 2. 3GPP TS23.501,2018.
[48] SMART N P. The exact security of ECIES in the generic group model[M]//Cryptography and Coding. Berlin Heidelberg: Springer 2001: 73-84.
[49] IETF. Elliptic curves for security[S]. IETF RFC 7748, 2016.
[50] SECG SEC 2. Recommended elliptic curve domain parameters[S], Certicom Research, 2010.
[51] BASIN D, DREIER J, HIRSCHI L, et al. A formal analysis of 5G authentication[C]//ACM Conference on Computer and Communications Security, 2018.
[52] ZHANG X, KUNZ A, SCHRÖDER S. Overview of 5G security in 3GPP[C]//Standards for Communications and Networking. IEEE, 2017.
[53] PRASAD, ANAND R, et al. 3GPP 5G Security[J]. Journal of ICT Standardization, 6.1 (2018): 137-158.
[54] Study on the security aspects of the next generation system[R]. 3GPP TR33.899, 2017.
[55] IMT-2020. 5G 网络安全需求与架构白皮书[R]. 2017.
IMT-2020. 5G Network security requirements and architecture white paper[R]. 2017.
[56] IETF RFC 3748. Extensible authentication protocol (EAP)[S]. 2004.
[57] 冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018(6).
FENG D G, XU J, LAN X. Research on 5G mobile communication network security[J]. Journal of Software, 2018(6).

[作者简介]

胡鑫鑫（1994-），男，湖北襄阳人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为 5G 网络安全。

刘彩霞（1974-），女，山东烟台人，国家数字交换系统工程技术研究中心副教授，主要研究方向为移动通信网络、新型网络体系结构。

刘树新（1987-）男，山东潍坊人，国家数字交换系统工程技术研究中心助理研究员，主要研究方向为复杂网络、网络信息挖掘。

游伟（1984-），男，江西丰城人，国家数字交换系统工程技术研究中心助理研究员，主要研究方向为密码学、移动通信网络。

乔康（1994-），男，四川成都人，国家数字交换系统工程技术研究中心硕士生，主要研究方向为区块域技术。