新空口场景下的安全认证协议设计与分析

作者姓名 马如慧

指导教师姓名、职称 冯登国、曹进 教授

申请学位类别 工学博士

学校代码 10701　　学　号 1715110417
分 类 号 TN91　　密　级 公开

西安电子科技大学

博士学位论文

新空口场景下的安全认证协议设计与分析

作者姓名：马如慧

一级学科：网络空间安全

二级学科（研究方向）：无

学位类别：工学博士

指导教师姓名、职称：冯登国、曹进 教授

学　　院：网络与信息安全学院

提交日期：2020年12月

Design and analysis of security authentication protocol in new air interface

A Thesis submitted to

XIDIAN UNIVERSITY

in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

in Cyber Security

By

Ma Ruhui

Supervisor: Feng Dengguo, Cao Jin Title:Professor

December 2020

西安电子科技大学
学位论文独创性（或创新性）声明

秉承学校严谨的学风和优良的科学道德，本人声明所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果；也不包含为获得西安电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同事对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文若有不实之处，本人承担一切法律责任。

本人签名：马如慧　　日　　期：2020.12.10

西安电子科技大学
关于论文使用授权的说明

本人完全了解西安电子科技大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权属于西安电子科技大学。学校有权保留送交论文的复印件，允许查阅、借阅论文；学校可以公布论文的全部或部分内容，允许采用影印、缩印或其它复制手段保存论文。同时本人保证，结合学位论文研究成果完成的论文、发明专利等成果，署名单位为西安电子科技大学。

保密的学位论文在____年解密后适用本授权书。

本人签名：马如慧　　导师签名：

日　　期：2020.12.10　　日　　期：2020.12.14

摘要

第三代合作伙伴计划（third Generation Partnership Project，3GPP）成立于1998年，从最初的通用移动通信系统网络，到长期演进（Long Term Evolution，LTE）网络、LTE网络的后续演进（LTE-Advanced，LTE-A）网络，再到当前主流发展的第五代移动通信技术（fifth Generation，5G）网络，3GPP已成长为全球最大的通信标准组织。为满足日益增长的用户通信需求，3GPP网络新空口引入了多种不用类型的实体和技术。首先，LTE-A网络中为了解决普通基站（evolved Node B，eNB）室内覆盖较弱的问题，引入了家庭基站（Home evolved Node B，HeNB），实现了家庭特色覆盖和业务需求。其次，由于5G网络支持高速传输，而高速传输最典型的场景就是高铁网络且高铁网络中数据传输遭受着严重的路径损耗等问题，为了给高铁网络中的用户提供平滑的通信体验，3GPP引入了车载移动中继节点（Mobile Relay Node，MRN）作为车载基站为列车上的用户终端提供稳定的网络服务。最后，为了实现全球网络覆盖，3GPP Rel-17引入了卫星接入技术，作为地面空口接入技术的有效补充。但是，这些新空口实体和技术的引入带来了一些新的安全和性能的挑战，需要进一步的研究和解决。

本文系统地研究了新空口实体和技术带来的不同的安全和性能问题，并提出了相应的解决办法。本文的主要贡献总结如下：

（1） 分析了LTE-A网络中多种类型的HeNB和eNB共存时的切换认证场景，指出了多种类型基站共存导致LTE-A网络终端移动切换场景变得异常复杂。此外，现存的切换认证方案存在大量的安全或性能缺陷，并不能满足当前LTE-A网络的需求。针对上述问题，基于椭圆曲线无证书签密技术，设计了一个终端统一切换认证方案。该方案可以适用于LTE-A网络中的所有移动场景，只需三次握手即可实现安全的切换认证，并且在不牺牲效率的前提下保证了多个强安全属性，包括相互认证、密钥协商以及隐私保护等。

（2） 分析了5G高铁网络中引入MRN后的切换认证场景，指出了现有3GPP标准中MRN的认证机制仍然无法为高速列车上的用户终端提供平滑的通信体验且甚至可能导致MRN切换失败以及由于MRN通过不安全的空口信道接入网络导致新的安全问题，例如易遭受窃听攻击、假冒攻击等问题。此外，现有的MRN的切换认证方案存在大量的安全或性能问题，例如无法实现相互认证或耗费较多切换开销等。针对上述问题，结合5G网络异构特性，基于聚合签名技术和高铁轨迹可预测机制，提出了两种基于固定路径的群组预切换认证方

案：方案FTGPHA1和方案FTGPHA2。方案FTGPHA1可以实现大部分安全属性且同时耗费较少的切换开销，而方案FTGPHA2可以在不牺牲效率的前提下实现健壮的安全属性。在这两个方案中，MRN可以在源基站的覆盖范围内提前与目标基站执行群组预切换认证过程，进而可为用户终端提供平滑的通信体验且避免切换失败等问题。

（3） 分析了5G网络中引入卫星接入技术后的接入认证场景，指出了卫星网络空口链路高度开放以及星地传输距离较远等特点导致卫星网络容易遭受各种各样的协议攻击以及用户终端认证时延过长等问题。此外，5G支持海量物联网设备（Internet of Things Device，IoTD）并发接入，而海量IoTD并发接入卫星网络且每个IoTD执行单独的接入认证过程会瞬时产生大量的信令开销，进而可能导致信令风暴等问题。针对上述问题，基于格理论密码学，提出了一种抗量子的接入认证方案。该方案包括两种认证协议：海量IoTD的并发接入认证协议和一个普通移动设备或者IoTD 的接入认证协议。在海量IoTD的并发接入认证协议中，海量IoTD构成一个临时群组执行群组认证过程以此克服信令风暴问题。此外，提出的两个协议可以实现较强的安全属性包括相互认证、条件匿名以及抵抗量子攻击和多种协议攻击等。

关键词：LTE-A， 5G， 空口， 认证， 家庭基站， 移动中继， 卫星接入技术

ABSTRACT

The third generation partnership project (3GPP) was founded in 1998, from the original universal mobile telecommunications system network to the long term evolution (LTE) network, LTE-Advanced (LTE-A) network, and then the current mainstream fifth generation (5G) network, 3GPP has become the largest communication standard organization in the world. In order to meet the increasing communication requirements of users, 3GPP network introduces a variety of new air interface entities and technologies. Firstly, in LTE-A network, in order to solve the problem of weak indoor coverage of ordinary evolved node B (eNB), the home evolved node B (HeNB) is introduced to realize the family characteristic coverage and service requirements. Secondly, since 5G network supports high-speed transmission, the most typical scenario of high-speed transmission is high-speed rail network and data transmission in high-speed rail network suffers from serious path loss and other problems. In order to provide smooth communication experience for users in high-speed rail network, 3GPP introduces mobile relay node (MRN) as on-board base station to provide stable network services. Finally, in order to achieve global network coverage, 3GPP Rel-17 introduces satellite access technology as an effective supplement to ground air access technology. However, the introduction of these new air interface entities and technologies has brought some new security and performance challenges, which need to be further investigated and solved.

This thesis systematically studies these different security and performance challenges brought by these new air interface entities and technologies, and puts forward the corresponding solutions. The manifold contributions of this thesis are summarized as follows:

(1) This thesis analyzes the handover authentication scenario in LTE-A network when multiple types of HeNB and eNB coexist, and points out that the coexistence of multiple types of base stations makes the handover scenario of LTE-A network extremely complex. In addition, these existing handover authentication schemes have a lot of security or performance defects, which cannot meet the needs of the current LTE-A network. To solve the above problems, we design a unified handover authentication scheme based on the elliptic curve certificateless signcryption technology. This scheme can be applied to all mobile scenarios in LTE-A network, only needs three handshakes to achieve secure handover authentication, and ensures multiple security properties without sacrificing efficiency, including mutual authentication, key agree-

ment, privacy preserving and so on.

(2) This thesis analyzes the handover authentication scenario introduced by MRN in 5G high-speed rail network, and points out that the existing authentication mechanism of MRN in 3GPP standard still cannot provide smooth user communication experience for user equipment and even may lead to MRN handover failure in high-speed rail network, and new security issues such as eavesdropping attacks, counterfeiting attacks and so on, arise due to MRN accessing the network through unsafe air interface channel. In addition, the existing MRN handover authentication schemes have many security or performance problems, such as unable to achieve mutual authentication or costing a lot of handover overheads. To solve the above problems, combined with the heterogeneous characteristics of 5G network and on the basis of the aggregate signature technology and the predictable mechanism of high-speed trajectory, we propose two fixed-trajectory group pre-handover authentication schemes: FTGPHA1 and FTGPHA2. FTGPHA1 can achieve most of the security properties and consume less handover overheads, while FTGPHA2 can achieve robust security properties without sacrificing efficiency. In the two proposed schemes, MRN performs group handover authentication with the next base station in advance within the coverage of the source base station, thus providing a smooth communication experience for the user equipment in high-speed rail network, avoiding MRN handover failure and other problems.

(3) This thesis analyzes the 5G network access authentication scenarios introduced by the satellite access technology and points out that the satellite network is vulnerable to various protocol attacks and the user equipment authentication delay is too long due to the highly open air interface and long transmission distance between satellite and ground. In addition, 5G supports the concurrent access of large-scale Internet of Things devices(IoTDs). Massive IoTDs concurrent accessing to satellite network and each IoTD performing its own access authentication process respectively will generate a lot of signaling overheads, which may lead to signaling storm and other problems. To solve these problems, we propose a quantum resistant access authentication scheme based on lattice cryptography. The scheme consists of two authentication protocols: access authentication protocol for massive IoTDs and access authentication protocol for a common mobile equipment or a single IoTD. In the access authentication protocol for massive IoTDs, massive IoTDs construct a temporary group to perform the group authentication process to overcome signaling storm and other problems. In

addition, the two protocols can achieve strong security properties including mutual authentication, conditional anonymity and resist against quantum attacks and multiple protocol attacks.

Keywords: LTE-A, 5G, Air interface, Authentication, Home base station, Mobile relay, Satellite access technology

插图索引

表格索引

符号对照表

符号	符号名称
q	大素数
Z	整数空间
Z^m	m维整数空间
Z_q	模q剩余类环
$Z_q^{n\times m}$	$n \times m$维的Z_q
$\boldsymbol{e}$	向量$\boldsymbol{e}$
$\boldsymbol{e_j}$	向量$\boldsymbol{e_j}$
e_j	向量$\boldsymbol{e}$的第j个元素
$\boldsymbol{A}$	矩阵$\boldsymbol{A}$
$\boldsymbol{A}^t$	矩阵$\boldsymbol{A}$的转置
$\boldsymbol{A}^{-1}$	方阵$\boldsymbol{A}$的逆
$\boldsymbol{A} \parallel \boldsymbol{B}$	矩阵$\boldsymbol{A}$和矩阵$\boldsymbol{B}$的串联
E	椭圆曲线E
G	循环群G
P	循环群的生成元
Λ	格Λ
$\|\cdot\|$	欧几里德范数
$\ll$	远小于
$\equiv$	同余
$\stackrel{?}{=}$	判断是否等于
$\oplus$	异或
$h()$	单向哈希函数

缩略语对照表

缩略语	英文全称	中文对照
3GPP	third Generation Partnership Project	第三代合作伙伴计划
3G	third-Generation	第三代移动通信技术
4G	fourth-Generation	第四代移动通信技术
5G	fifth-Generation	第五代移动通信技术
5G-AKA	5G Authentication and Key Agreement	5G认证与密钥协商协议
5G-GUTI	5G Globally Unique Temporary Identifier	5G网络全球唯一临时终端标识
AES	Advanced Encryption Standard	高级加密标准
AKA	Authentication and Key Agreement	认证与密钥协商
AMF	Access and Mobility Management Function	接入和移动管理实体
ARFCN	Absolute Radio Frequency Channel Number	绝对频点号
BAN	Burrows-Abadi-Needham	逻辑分析工具
CHTT	Collaborative Handover Trigger Threshold	协同切换触发门限
CMA	Chosen Message Attack	选择消息攻击
CSG	Closed Subscriber Group	封闭用户组
DeNB	Donor eNB	宿主4G基站
DgNB	Donor gNB	宿主5G基站
DH	Diffie-Hellman	DH算法
DLP	Discrete Logarithm Problem	离散对数问题
D-SDN	Donor Software Defined Networking controller	软件定义网络控制器
EAP-AKA	Extensible Authentication Protocol-AKA	扩展认证协议-认证与密钥协商协议
EAP-AKA’	Improved EAP-AKA	改进的EAP-AKA
ECDH	Elliptic Curve Diffie-Hellman	椭圆曲线DH算法
ECDHP	Elliptic Curve Diffie-Hellman Problem	椭圆曲线DH问题
ECDLP	Elliptic Curve Discrete Logarithm Problem	椭圆曲线离散对数问题
ECDSA	Elliptic Curve Digital Signature Algorithm	椭圆曲线数字签名算法
eNB	Evolved Node-B	演进的基站
EPC	Evolved Packet Core	演进的分组核心网
E-UTRAN	Evolved UTRAN	演进的UTRAN

FADL	Frequency ARFCN-DL	下行链路绝对频点号
FTGPHA	Fixed-Trajectory Group Pre-Handover Authentication scheme	固定路径群组预切换认证方案
gNB	NR Node B	NR基站
GS	Ground Station	地面站
GSA	Global mobile Suppliers Association	全球移动设备供应商协会
GUTI	Globally Unique Temporary Identifier	全球唯一临时终端标识
HeNB	Home evolved Node B	演进的家庭基站
HSS	Home Subscriber Server	归属签约服务器
HT	Handover Ticket	切换凭证
HTT	Handover Trigger Threshold	切换触发门限
ID	Identity	身份标识
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IoT	Internet of Things	物联网
IoTD	Internet of Things Device	物联网设备
ISIS	Inhomogeneous Small Integer Solution	非齐次小整数解
ITU	International Telecommunications Union	国际电信联盟
KGC	Key Generation Center	密钥生成中心
LEO	Low Earth Orbit	近地轨道
LTE	Long Term Evolution	长期演进技术
LTE-A	LTE-Advanced	LTE技术的后续演进
MAC	Message Authentication Code	消息认证码
ME	Mobile Equipment	移动终端
MME	Mobility Management Entity	移动性管理实体
MRN	Mobile Relay Node	移动中继节点
MTC	Machine Type Communications	机器类型通信
NCC	Network Control Center	网络控制中心
NH	Next Hop	下一跳
NIST	National Institute of Standards Technology	国际标准技术研究机构
NP	Non-deterministic Polynomial	非确定多项式
NR	New Radio	新空口
PCI	Physical Cell ID	物理小区标识
RSA	Rivest-Shamir-Adleman cryptosystem	RSA密码体系

S-GW	Serving GateWay	服务网关
SIS	Small Integer Solution	小整数解
sUF	strongly UnForgeable	强不可伪造性
SUPI	SUbscription Permanent Identifier	用户永久身份标识
TST	Terrestrial-Satellite Terminals	陆地-卫星终端
UE	User Equipment	用户终端
UMTS	Universal Mobile Telecommunications System	通用移动通信系统
UTRAN	UMTS Terrestrial Radio Access Network	UMTS陆地接入网络

目录

第一章　绪论

1.1　研究背景

第三代合作伙伴计划（third Generation Partnership Project，3GPP）委员会于2004年在Rel-8中启动了长期演进技术（Long Term Evolution，LTE）项目[1]。相比于以往的第三代移动通信技术（third-Generation，3G），LTE网络带宽更高且能够传输更高质量的视频及图像。为了更好的满足用户通信需求，3GPP于2008年在Rel-10启动了LTE技术的后续演进（LTE-Advanced，LTE-A）项目[1]。LTE-A网络支持LTE后向兼容，可达500Mbps峰值速率以及最大100MHz带宽。此外，LTE-A网络中引入了家庭基站以提供室内覆盖等特性。LTE-A是国际电信联盟（International Telecommunications Union，ITU）确定的第四代移动通信技术（fourth Generation，4G）标准之一。4G网络的出现，使得网络数据传输速率有了质的飞跃。根据全球移动设备供应商协会（Global mobile Suppliers Association，GSA）分析报告[2]，到2019年底，全球共有52.7亿个LTE用户，占全球移动用户总数的57.7%；截至2020 年2 月底，有788家运营商推出了商用LTE网络；138个国家启动/部署了311个LTE-A网络；超147个国家的348家运营商正在投资LTE-A网络。根据GSA预测，到2022年底，4G 用户在全球总移动用户中的占比将超过61%。4G用户的不断增长也带动了移动互联网用户数量的猛增。而随着移动互联网用户数量的增多，用户对于互联网应用的需要也越来越高。

为了应对未来移动数据流量爆炸性的增长、海量设备的连接、各类新兴业务和应用场景的不断涌现，第五代移动通信技术（fifth-Generation，5G）应运而生。2015年，ITU定义了5G三大典型应用场景：增强型移动宽带、超可靠低延迟通信、大规模机器类型通信[3]。其中，增强型移动宽带是传统4G功能的升级，主要实现超高的用户体验速度以及超高的用户密度。此外，考虑到目前的4G 等技术在移动性和宽带性上都无法满足超高速移动宽带的要求，增强型移动宽带场景中还指出了在高速移动场景下，需为用户提供与低速移动场景下的一致体验等特性。超可靠低延迟通信主要针对自动驾驶、远程医疗等场景。大规模机器类型通信主要满足大量机器类型通信设备、传感器等物联网领域的通信要求。3GPP于2016年在Rel-15中正式启动了5G标准化研究工作。Rel-15 初步满足了5G网络增强移动宽带以及部分低时延高可靠场景等基本要求。Rel-15作为第一阶段5G的标准版本于2019年3月冻结。为进一步完善5G网络需求，3GPP于2018年6 月启动了Rel-16 标准制定工作。Rel-16侧重于超可靠低时延通信、工业物联网、移动性增强等方面，并进一步优化已有Rel-15相

关功能[4]。Rel-16作为第二阶段5G的标准版本于2020年7月冻结，这标志着5G第一个演进版本标准完成。2020年7月，3GPP系的5G标准正式被接受为ITU 5G技术标准。至此，5G三大场景核心支持标准已准备就绪。2020年5G第一阶段标准启动大规模部署，进入全面商用。而在5G商用实践的同时，5G网络的构建仍在继续。Rel-16标准基本上满足了用户终端在陆地网络的基本通信需求，但是还未实现全方位、立体化多域覆盖等特性。因此，为进一步提升5G网络能力，3GPP于2019年12 月启动了5G第三阶段Rel-17标准制定工作。Rel-17标准一方面是对已有的Rel-15/Rel-16进行了全方位的增强和优化，另外一方面是提出了一些新的业务和能力需求，例如引入了卫星网络作为非陆地网络新空口接入技术等。

在5G网络商用与继续构建的同时，4G网络的发展也仍在继续。在2019年12月13日“中国5G经济研讨会”上发布的《中国5G经济报告2020》中提到，5G不会在短期内完全改变或颠覆电信领域或其他行业，预计未来10年4G仍将与5G长期共存[5]。4G移动通信技术仍然是我国移动业务的主要承载，由于4G网络全覆盖的应用优势，其应用能够满足当前大部分的业务需求[6]。在未来几年4G网络将会继续扩大市场份额，甚至会长时间占据市场主导地位。事实上，4G网络将在5G网络扎根之时起到补充甚至支撑的作用[7]。因此，4G与5G网络协同发展是当前的主流趋势。

为满足日益增长的用户通信需求，3GPP 4G与5G网络空口引入了多种不用类型的实体和技术，而这些新空口实体和技术的引入带来了一些新的安全和性能的挑战，需要进一步的研究和解决。本文重点分析了以下几种新空口实体和技术。

（1）LTE-A网络家庭基站的引入

LTE-A网络架构主要包括两部分内容：接入网（Evolved UMTS Terrestrial Radio Access Network，E-UTRAN）以及核心网（Evolved Packet Core，EPC）。接入网中有大量的基站，核心网中有一个归属网络服务器（Home Subscriber Server，HSS）以及多个移动性管理实体（Mobility Management Entity，MME）等[8]。在LTE-A接入网络中，主要有两种类型的基站，普通基站（evolved Node B，eNB）以及家庭基站（Home evolved Node B，HeNB）。HeNB不同于传统的室外普通eNB，主要用于增加室内网络的覆盖范围，解决普通eNB室内覆盖较弱的问题。由于用户终端（User Equipment，UE）与基站是通过不安全的无线空口信道连接，当UE从源基站移动至目标基站的覆盖范围时，为享受连续安全的网络服务，UE必须与目标基站进行切换认证。但是，HeNB的引入导致现有终端切换认证方案存在以下问题：

首先，由于HeNB的存在，UE移动切换场景变得异常复杂。不同的移动场景需要执行不同的切换认证过程。切换认证的多样性增加了整个LTE-A网络的复杂性。其次，由于UE与基站是通过不安全的无线空口信道进行连接，攻击者可能在空口信道上发起窃听、拦截、假冒等攻击。然后，UE通常功率和处理能力受限导致无法部

署较为复杂的密码学算法。综上所述，在LTE-A异构网络中，提出一种统一、安全、高效的终端切换认证机制是至关重要的。

（2）高铁网络移动中继的引入

5G网络支持高速传输，而高速传输最典型的场景就是高铁网络。IMT-2020推进组指出，即使在500km/h的速度下，5G网络仍能向用户提供平滑的通信体验[9]。因此，如何保障高铁网络用户终端的通信服务质量是当前5G研究的热点。在高铁网络中，由于高铁的高速移动性，数据传输遭受着严重的路径损耗、多普勒频移等问题[10]。另外，当列车从一个基站驶向另外一个基站时，列车上的海量UE 会并发、频繁激活切换认证过程，瞬时产生大量的通信开销和信令开销，进而可能导致切换失败等问题[11]。为了解决上述问题，3GPP提出了采用移动中继（Mobile Relay Node，MRN）作为车载基站为列车上的用户终端提供稳定的网络服务[12, 13]。MRN提供两种功能：UE的功能和基站的功能。在初始入网和切换的过程中，MRN作为普通UE接入网络，随后辅助列车上的海量UE 接入5G 网络。由于MRN可以聚合列车上所有UE的消息，因此可以很大程度地降低信令开销。此外，由于UE与MRN之间距离相对较固定且MRN是有源供电，所以MRN可为UE提供较为稳定的网络服务。但是，MRN的引入存在以下问题：

- 由于MRN是通过不安全的空口信道接入5G 核心网络，MRN的引入会带来新的安全问题，例如易遭受窃听攻击、假冒攻击等。所以为保障MRN安全可靠的接入5G网络，MRN必须与5G网络完成认证。

- 根据3GPP标准，当列车刚进入目标基站的覆盖范围后，MRN需先与目标基站执行切换认证过程，再辅助列车上的用户终端接入网络，即此时用户终端仍需依赖于源基站接入5G网络，但是由于列车的高速运行，列车上的用户终端高速偏离源基站，也就是说在MRN执行切换认证的过程中，列车上用户接收到的数据信号快速变弱，无法提供平滑的用户通信体验。

- 根据3GPP标准[13–15]，终端切换过程需依赖于源基站且MRN的切换过程与普通终端的切换过程一致。但是，在MRN切换过程中，列车高速偏离源基站，源基站可能无法接收到MRN发送的切换请求消息且MRN也无法接收到源基站发送的切换响应消息，进而导致切换失败等问题。

- MRN仍然遭受着频繁切换的问题[11]。由于列车高速移动，列车在某个基站的逗留时间可能极短，MRN无法与该基站完成一次完整的切换过程，进而也导致MRN切换失败等问题。

因此，提出适用于高铁网络中MRN作为终端的安全、无缝、快速的切换认证机制是必不可少的。

（3）卫星接入技术的引入

为了实现全球网络覆盖，3GPP等国际组织已经将卫星网络列为5G接入方式之一[16]，作为地面空口接入技术的有效补充。我国科技部也已于2019年启动了卫星通信与5G地面移动通信融合技术的研发工作。卫星网络能够克服地面地势、海拔等自然因素、部署网络跨度大和部署成本高等影响，为用户提供无区域阻隔、成本友好的全球通信和数据采集服务。但是，卫星接入技术的引入在性能和安全方面也带来一些新的问题。

首先，由于卫星网络空口链路高度开放，卫星网络容易遭受各种各样的协议攻击，例如假冒攻击和中间人攻击等[17, 18]。其次，由于卫星与地面距离较远，即使是近地轨道（Low Earth Orbit，LEO）距离地面也至少500公里[19]，卫星与地面之间传输时延过长。最后，5G支持超高密度的海量物联网设备（Internet of Things Device，IoTD）并发接入网络，而海量IoTD并发接入卫星网络且每个设备均独自执行认证协议时，会瞬时产生大量的通信和信令开销，进而导致信令风暴、关键节点拥塞故障等问题。因此，针对海量IoTD设计一个安全高效的接入卫星网络的认证协议是十分必要的。与此同时，为了提供更健壮的安全属性，针对单个IoTD或者单个用户设备（Mobile Equipment，ME）设计安全高效的接入卫星网络的认证协议也是至关重要的。

1.2 研究现状

针对3GPP网络空口引入新的实体和技术场景下安全认证机制方面，目前工业界已制定一些标准且学术界已有一些相关论文。

（1）LTE-A网络中终端的切换认证机制

根据3GPP标准[20]，eNB和HeNB之间的移动场景主要包括以下三种类型：基于X2的切换、基于S1的切换至混合式HeNB或封闭式HeNB以及基于S1的MME间切换。基于X2的切换是指从eNB或任意类型的HeNB切换至eNB或开放式HeNB。基于S1的切换至混合式HeNB或封闭式HeNB中，MME需要检查UE是否是目标混合/封闭式HeNB的成员。基于S1的MME间切换则需源MME与目标MME同时参与完成UE权限的鉴权。但是，当前的切换认证标准仍然存在安全和性能缺陷，例如隐私泄露、无法提供完美前向、后向安全等问题。与此同时，基于S1的切换过程仍然需要终端与源基站和MME进行多轮信息交互，产生了较多的通信开销。此外，终端在不同的移动场景需要执行不同的切换认证过程，切换认证的多样性将增加整个系统的复杂性。

近年来，学术界已经提出了大量的无线网络中的切换认证方案[21–25]。2007年，Kim等人[21]基于身份公钥密码学机制提出了一个快速的漫游认证方案。该方案可以实现相互认证且同时耗费较少的通信开销。但是该方案中并未提及如何协商会话密钥以保护未来通信数据的机密性，且该方案耗费了较多的计算开销。Jing等人[22]提出了一个隐私保护的切换认证方案且声称该方案基于椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）和椭圆曲线Diffie-Hellman问题（EllipticCurveDiffie-HellmanProblem，ECDHP）可以实现完美前向、后向安全，但是，通过对方案的详细分析，当终端私钥泄露的情况下，攻击者可以从终端公开传输的签名中推导出随机数，进而根据随机数算出会话密钥，因此，该方案并不能实现完美前向、后向安全。Choi等人[23]和Cao等人[24]分别基于代理签名机制提出了两个切换认证方案。但是，同方案[22]类似，文献[23, 24]中的方案也不能实现完美前向、后向安全。另外，文献[24]中的方案不能保护用户的隐私信息。2017年，Qiu等人[25]提出了一个改进的代理签名切换认证方案。该方案可以实现完美前向、后向安全，但是该方案不能保护用户的隐私信息。另外，在文献[22–25]中，终端的私钥完全依赖于服务器端，例如HSS。一旦攻击者攻陷了用户终端与服务器之间的信道，攻击者可以获取所有终端的私钥。

终端隐私信息的泄露可能会严重损害用户的正常生活，窃取用户资产，甚至威胁用户的生命安全，而上述方案[21–25]并未实现安全的隐私保护。此外，若切换认证过程中的计算开销较大则会直接影响到终端切换认证时延，进而导致终端网络通信质量差等问题，而上述方案[21]采用了多个双线性映射操作，无疑会产生大量的计算开销。此外，上述方案[22–25]存在完全依赖于单点服务器等问题，而无证书认证方案可以很好的规避此问题。因此，研究LTE-A网络中低开销隐私保护的无证书切换认证方案是非常有意义的。

（2）高铁网络中移动中继的切换认证机制

根据3GPP标准[13]，MRN的切换步骤与UE的切换步骤[14, 15]一致。但是，3GPP定义的UE的切换步骤[14, 15]存在一些安全漏洞，例如无法实现前后密钥分离以及不能抵抗重放攻击等[26]。此外，3GPP定义的终端的切换步骤严格依赖于源基站，而高铁快速运行过程中源基站信号快速变弱，可能导致MRN切换失败以及无法为高铁用户终端提供平滑通信体验等问题。

近年来，学术界针对MRN只提出了少量的切换认证方案[10, 11, 27–31]。Kong等人[10]基于代理再加密技术提出了一个LTE-A 网络安全切换密钥协商方案。在该方案中，UE采用MME的公钥加密初始生成的会话密钥获得密文，随后，MRN将UE的密文用目标eNB的公钥再次加密。因此，目标eNB可以在无源MME参与的情况下解密密文。该方案可以成功完成会话密钥的协商以及保证会话密钥的前后分离特性。但是，该

方案不能提供完美前向、后向安全且不能抵抗缺乏密钥确认攻击等，以及该方案耗费了大量的计算开销。Pan[11]等人针对MRN提出了一个增强的切换认证方案。该方案与LTE-A网络协议兼容。但是该方案重点关注切换开始的测量过程，整个切换过程除了测量过程都与LTE-A完全相同，因此继承了LTE-A网络的安全缺陷。Tian等人[27]提出了一个无缝切换认证方案。在该方案中，为了减少切换开销，每个UE的切换请求消息由接入点汇聚后转发给MRN，MRN代表车上的所有UE与基站执行切换认证过程。Huang等人[28]提出了一个LTE-A网络MRN快速切换认证方案。在该方案中，为了提高切换性能，包含在预切换消息中的文本信息以及位置信息等内容被提前发送给目标eNB。一旦MRN 到达目标基站的覆盖范围，目标基站启动切换过程，以此减少切换执行时间。但是，文献[27, 28]中的方案并未考虑认证安全。Cao 等人[29]基于路径预测设计了一个切换认证方案。在该方案中，部署在车辆运行轨迹周边的eNB构成一个eNB群组，且共享一个组密钥。该方案可以成功实现MRN 和目标eNB之间的相互认证和密钥协商过程且耗费合理的开销。但是，该方案并没有实现一些重要的安全属性，例如隐私保护以及完美前向、后向安全等。Cao等人[30]针对MRN提出了一个组到路由（group-to-route）切换认证方案。通过该方案，所有路边基站（Donor Evolved Node-B，DeNB）构成一个eNB群组，且车上所有MRN构成一个MRN群组。源DeNB为每个MRN生成切换凭证（Handover Ticket，HT），随后MRN和目标DeNB 利用HT实现相互认证和密钥协商过程。但是，该方案并未实现前后密钥分离、完美前向、后向安全、匿名性以及不可链路性。Haddad等人[31]介绍了一个LTE-A网络隐私保护MME间的组切换认证方案。通过该方案，每个用户拥有大量的一次性公私钥对，且每次选取其中一个公私钥对生成签名。MRN汇聚所有的签名消息并将其转发给eNB。该方案可以提供匿名认证且保护用户隐私信息。但是，该方案由于执行了多个双线性映射操作而耗费了大量的通信开销和计算开销。

上述方案[10, 11, 27–31]均是移动中继到达目标基站的覆盖范围内，再启动切换认证过程。但是在此过程中，由于列车上的移动中继高速偏离源基站，源基站信号较差，不可能依赖于源基站进行稳定的数据通信，且由于目标基站并未成功接入也无法依赖于目标基站进行稳定的数据通信，所以在切换认证过程中，即使切换认证时延较短，这些方案均无法提供稳定连续的网络通信服务。此外，隐私泄露可能会严重损害用户的正常生活，因此确保隐私数据的机密性至关重要，但是上述方案[10, 11, 27–30]存在未能实现隐私保护、完美前向、后向安全、前后密钥分离等隐私属性。因此，研究适用于高铁网络移动中继的可实现隐私机密性的同时且可为终端提供平滑的通信体验的切换认证方案是非常重要的。

（3）5G卫星网络中终端接入认证机制

近些年来，学术界的研究者已经提出了多个卫星网络认证方案[32–41]。Hwang等

人[32]，Chang等人[33] 和Chen等人[34] 分别提出了相互认证方案。这些方案由于只采用了一些简单的哈希、异或以及对称加密/解密操作，耗费了较少的计算开销。但是文献[32, 33]中的方案并未实现一些重要的安全属性，例如隐私保护、数据机密性、以及会话密钥的独立性等。此外，Chen等人在文献[35]中指出文献[34]中的方案不能保护用户隐私，实现机密性以及抵抗假冒攻击。随后，Chen等人[35]改进了文献[34]中的方案，并且提出了一些新的相互认证方案。该方案可以降低UE 侧的计算开销，防止用户隐私泄露以及利用签名技术保障了消息的完整性。在文献[32–35]中的方案，地面网络控制中心（Network Control Center，NCC）需要完整参与每个UE 的接入认证过程，导致生成大量的计算开销。为了减少NCC侧的计算负荷，Zhang等人[36] 和Zheng 等人[37]分别提出了一个有效的认证方案。在文献[36]中的方案，UE与目标卫星可以在无NCC的参与下直接完成认证。此方案利用自认证公钥密码学技术可以避免系统中心被破坏，所有私钥都暴露的风险。但是，在该方案中，会话密钥是在UE与卫星之间协商，由于卫星的存储能力受限[42]不可能存储过多UE 的会话密钥。另外，由于卫星通过不安全的无线链路接入地面站（Ground Station，GS），不诚实的卫星可能窃听用户的通信数据。通过文献[37]中的方案可以有效减少NCC侧的计算开销，但是该方案容易遭受各种各样的攻击，例如身份欺骗攻击，恶意服务请求攻击以及拒绝服务攻击等[38]。为了克服方案[37]中的安全缺陷，Zhao等人[38]提出了一个新的相互认证协议。在该协议中采用NCC的长期私钥用以抵抗身份欺骗攻击，通过验证用户身份标识信息来抵抗恶意服务请求攻击，并且利用自更新和超时重传机制来克服拒绝服务攻击。但是，对于文献[32–35, 37, 38]中的方案，由于用户在每次访问认证过程中仍然需要等待地面节点的回复，因此存在无法容忍的认证延迟。

Meng等人[39]，Xue等人[40]以及Yang等人[41]分别提出了一个安全的卫星网络认证方案。在这些方案中，具有星载处理能力的卫星节点可以替代地面节点与UE执行接入认证过程，即卫星可以直接认证UE而无需地面节点的参与。因此，可以有效减少卫星与地面节点之间的交互次数，进而降低认证时延。与此同时，为了降低卫星的存储负荷以及防止恶意卫星节点窃听用户通信数据，UE和GS协商会话密钥，以保证空口无线链路通信的机密性。但是，文献[39, 40]中的方案并未实现不可链路性以及完美前向、后向安全，且文献[41]中的方案由于使用了多个点乘和双线性映射操作耗费了大量的计算开销。

综上所述，所有现有方案都是针对单个实体而设计的，无法避免海量设备并发接入卫星网络时导致的信令冲突问题。此外，星地距离较远，交互次数过多会导致认证时延过长等问题，而文献[32–35, 37, 38]中的方案存在与地面交互次数过多导致认证时延过长等问题。另外，确保终端隐私安全至关重要，而文献[39, 40]均未实现不可链路性以及完美前向、后向安全。此外，为了提供更可靠的安全保护，还应考虑针对单个

实体的接入认证方案。因此，研究适用于5G卫星网络的可避免信令冲突的海量终端并发接入和单个实体接入的与地面交互次数较少的安全认证方案是十分必要的。

1.3 研究内容与创新点

1.3.1 研究内容

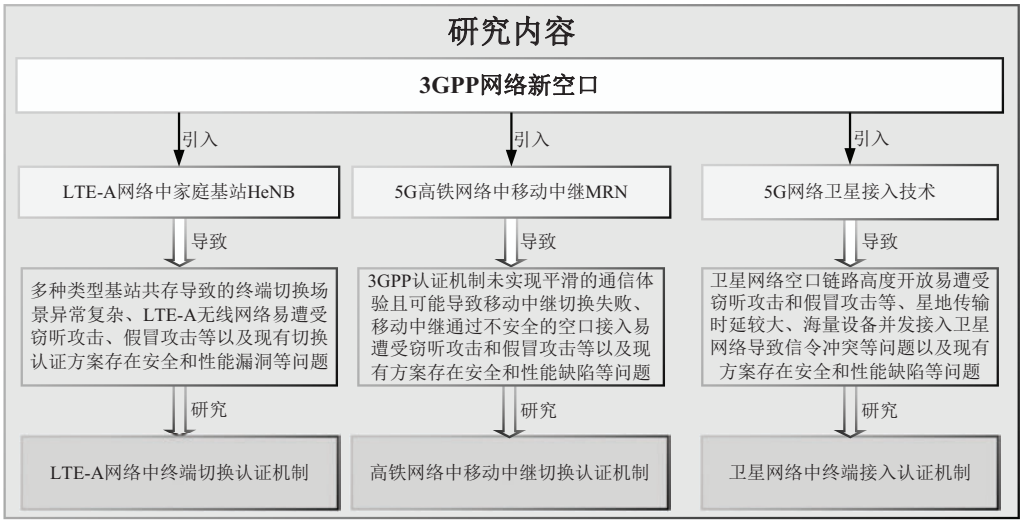


图 1.1 研究内容

如图1.1所示，本论文主要针对3GPP网络新空口引入新实体和技术后带来的安全和性能问题，研究适应于新空口场景下的安全认证机制，为当前主流的3GPP网络提供安全支撑。研究内容具体包括以下三个方面：

（1）LTE-A网络中终端的切换认证机制研究

针对LTE-A网络中多种类型基站共存导致的终端切换场景异常复杂以及现有切换认证方案存在各种各样的安全和性能漏洞等问题，研究适用于LTE-A网络所有移动场景的终端切换认证方案，基于椭圆曲线无证书签密机制实现终端侧与基站侧的双向认证，采用签密算法保障终端隐私数据的机密性，利用椭圆曲线Diffie-Hellman（Elliptic Curve Diffie-Hellman，ECDH）算法协商会话密钥以保护通信数据，降低终端切换认证复杂度，保障终端统一、安全、高效地接入LTE-A异构网络。

（2）5G高铁网络中移动中继的切换认证机制研究

针对5G高铁网络中MRN引入后当前3GPP定义的MRN的切换认证机制仍然无法为用户提供平滑的通信体验、MRN切换失败、新的安全问题例如假冒攻击、中间人攻击等，以及现有方案存在安全和性能缺陷等问题，研究适用于高铁网络MRN的切换认证方案，结合群组认证机制以进一步减少认证开销，利用椭圆曲线聚合签名机制降低通信开销，基于高铁和基站轨迹可预测机制实现MRN在源基站的覆盖范围内

提前与目标基站完成切换认证过程，进而为高铁用户提供平滑的通信体验。

（3）5G卫星接入网络中终端的接入认证机制研究

针对5G网络中卫星接入技术的引入导致的终端认证时延过长、海量IoTD并发接入卫星网络导致信令冲突、新的安全问题例如窃听攻击和假冒攻击等，以及现有方案存在各种各样的安全漏洞，耗费了大量的计算开销以及存在不可容忍的认证时延等问题，研究适用于5G卫星网络终端的接入认证方案，减少星地交互次数，降低星地认证时延，采用群组认证机制减少信令开销，保障单个实体或海量IoTD并发安全地接入卫星网络。

1.3.2　创新点

本论文的创新工作主要体现在以下三个方面：

（1）针对LTE-A网络中多种类型基站共存导致的终端切换场景异常复杂等问题，基于无证书签密技术提出了适用于LTE-A异构网络的隐私保护切换认证方案。该方案只需三次握手就可以实现安全的切换认证，并且在不牺牲效率的前提下提供健壮的安全属性。

（2）针对高铁网络中MRN引入导致的新的安全问题以及当前3GPP定义的MRN的切换认证机制仍然无法为用户提供平滑的通信体验且可能导致切换失败等问题，基于聚合签名技术和高铁与基站轨迹可预测机制提出了适用于MRN的群组预切换认证方案。在该方案中，5G核心网软件定义网络控制器D-SDN可以提前获取列车的轨迹信息，进而可基于轨迹预测机制提前决策出MRN群组即将要接入的目标基站，协助MRN与目标基站提前完成切换认证过程，为终端提供平滑的用户通信体验。

（3）针对5G网络中卫星接入技术的引入导致的新的安全问题、星地认证时延过长以及海量IoTD并发接入卫星网络导致信令冲突等问题，基于格理论密码学提出了适用于海量IoTD的并发接入认证方案以及适用于单个ME或IoTD的接入认证方案。在该方案中，海量IoTD构成一个临时群组执行群组接入认证过程以此克服信令冲突问题。通过利用提出的半聚合签名机制以及会话密钥协商机制，提出的群组方案可以有效降低传输负荷。

1.4　目标和贡献

针对新空口场景中面临的三种新的安全挑战，本文分别设计了安全高效的认证方案。本文主要贡献如下:

（1）针对LTE-A网络中多种类型基站共存导致的切换场景异常复杂等问题，提出了一种基于无证书签密技术的隐私保护切换认证方案。与其他现有方案相比，该

方案只需三次握手就可以实现安全的切换认证，并且在不牺牲效率的前提下保证了多个安全属性，包括相互认证、密钥协商、完美前向、后向安全、隐私保护以及可以克服密钥托管问题等，且该方案可以适用于LTE-A异构网络中的所有移动场景。形式化验证工具Proverif、逻辑分析工具（Burrows-Abadi-Needham，BAN）以及非形式化安全分析充分证明了提出的方案可以提供健壮的安全属性。

（2）针对高铁网络中MRN引入导致的新的安全问题以及当前3GPP定义的MRN的切换认证机制仍然无法为用户提供平滑的通信体验等问题，提出了两个群组预切换认证方案FTGPHA1 和FTGPHA2。在提出的两个方案中，同一列车上的多个MRN构成一个MRN群组。由于列车轨迹信息和基站位置信息通常是固定的，核心网软件定义网络控制器可以提前获取列车的轨迹信息，进而提前决策出MRN群组即将要接入的目标基站。在软件定义网络控制器的辅助下，MRN群组可以提前在到达目标基站覆盖范围前与目标基站执行群组预切换认证与密钥协商过程，因此，MRN的切换认证时延可以被忽略。另外，考虑到列车在某基站逗留时间可能极短，无法完成一个切换认证过程的问题，提出的两个方案中另外考虑了协同切换认证机制，以进一步减少通信和计算开销。方案FTGPHA1 是一个轻量级的预切换认证协议，它可以实现大部分安全属性且同时耗费较少的信令、通信和计算开销，而方案FTGPHA2是一个安全的预切换认证协议，它可以实现健壮的安全属性包括相互认证、密钥协商、完美前向、后向安全、匿名性、不可链路性、前后密钥分离以及抵挡多种协议攻击。与此同时，FTGPHA2耗费合理的切换开销。

（3）针对5G网络中卫星接入技术的引入导致的新的安全问题、终端认证时延过长以及海量IoTD并发接入卫星网络导致信令冲突等问题，提出了一个统一、安全、高效的基于格的接入认证方案。该方案针对海量IoTD和单个ME或单个IoTD提出了两种不同的协议：海量IoTD的接入认证协议以及单个ME/IoTD的接入认证协议。在海量IoTD的接入认证协议中，海量IoTD构成一个临时群组执行群组认证过程以此克服信令冲突问题。通过利用提出的半聚合签名机制以及会话密钥协商机制，提出的群组方案可以有效降低传输负荷。另外，提出的方案可以快速完成地面站与每个IoTD之间的密钥协商。可证明安全分析、BAN逻辑分析以及非形式化安全分析全方位证明了提出的两个协议可以提供健壮的安全属性。此外，与其他方案在信令开销和传输开销方面的对比结果显示提出的方案可以明显降低信令开销和传输开销。

1.5 组织结构

第一章，介绍了本论文的研究背景，描述了本论文的研究现状，进而阐述了本论文的研究内容与创新点、目标和贡献以及本论文的组织架构。

第二章，描述了本论文用到的一些基础知识，包括基本密码学原语的介绍以及

论文中用到的协议安全分析工具的介绍。基本密码学原语中则介绍了椭圆曲线密码学以及格理论密码学的基础概念。协议安全分析工具中则主要介绍了两个形式化验证工具Proverif和Tamarin以及一个逻辑分析工具BAN。

第三章，针对LTE-A异构网络，提出了一个终端切换认证方案，保障LTE-A异构网络中的终端可以统一、安全、高效的接入网络。

第四章，针对高铁网络，提出了两个群组预切换认证方案。其中，针对资源受限，用户性能较差以及安全性需求较低的场景，基于当前3GPP 5G认证与密钥协商协议（5G Authentication and Key Agreement，5G-AKA）/改进的扩展认证协议-认证与密钥协商协议（Improved Extensible Authentication Protocol-AKA，EAP-AKA'）提出了一个轻量级预切换认证方案。而针对用户性能较强，安全需求较高以及通信资源较为充裕的场景，基于椭圆曲线密码学中的聚合签名技术提出了一个强安全预切换认证方案。

第五章，针对卫星网络，提出了两个认证方案。其中，针对海量IoTD并发接入卫星网络场景，基于格理论密码学中的小整数解困难问题设计了群组接入认证方案。而针对单个ME或单个IoTD接入卫星网络场景，同样基于格理论密码学中的小整数解困难问题设计了单个实体接入认证方案。

第六章，总结了论文的工作内容以及对后续工作的展望。

第二章　基础知识

2.1　基本密码学原语

传统数论的密码学方案是基于某个数学难题的，例如基于有限域上离散对数问题（Discrete Logarithm Problem，DLP）的密码学方案ELGamal，基于椭圆曲线上离散对数问题的椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA），以及基于大整数分解的RSA算法（Rivest-Shamir-Adleman cryptosystem，RSA）等。基于传统数论的密码学方案是当前学术界的主流。然而，在未来，大规模量子计算机的部署导致基于传统数论的公钥密码系统变得不再安全，特别是这些基于大整数分解困难问题的密码学方案，例如RSA，ELGamal以及ECDSA等[43]。因此，基于抗量子密码学的研究也逐渐成为当前的研究核心。截止目前，学术界公认的抗量子的密码学方案主要包括基于格的密码学方案、基于编码的密码学方案、基于哈希函数的密码学方案以及基于多元多项式的密码学方案等[43]。

在本论文中，首先，基于椭圆曲线密码学上的无证书签密机制提出了一个适用于LTE-A网络的终端接入认证方案。然后，分别基于对称密码学和椭圆曲线密码学上的聚合签名机制提出了两种移动中继的群组切换认证方案。最后，基于格理论密码学中的小整数解困难问题提出了一个抗量子的终端接入认证方案。对称密码学方案较为简单，此处不做过多介绍，本小节，主要介绍椭圆曲线密码学以及格理论密码学的相关概念。

2.1.1　椭圆曲线密码学概述

椭圆曲线密码学是有限域F_p上的公钥密码体制。椭圆曲线公钥密钥学最早是由Miller和Koblitz等人各自独立在1985年和1987年提出[44, 45]。定义在有限域$GF(p)$上的椭圆曲线的方程是：$y^2 = (x^3 + a\,x + b)\,mod p$，其中$p$为素数，$a$和$b$满足：$4a^3 + 27b^2 \neq 0\,mod p$ [46]。满足上述方程的整数对(x, y)就是椭圆曲线上的点。有限域上的椭圆曲线主要有两种运算，点加运算和点乘运算。点加运算：对于椭圆曲线上的任意两点P和Q进行加法运算可得点$R = P + Q$。点乘运算：椭圆曲线上的点P乘以整数k，即$kP = P + P + ... + P$，其意义为计算kP需要对点P执行$k - 1$次点加运算。

椭圆曲线密码学的安全性基于如下两个公认的难解问题，迄今为止，学术界仍未找到有效的算法来破解此问题。

（1）椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）：P和Q是椭圆曲线上的两个点。给定点P和整数k，根据等式$Q = kP$，很容易计算

出Q。但是，给定点P和Q，计算整数k是困难的。

（2）椭圆曲线Diffie-Hellman问题（Elliptic Curve Diffie-Hellman Problem，ECDHP）: 给定椭圆曲线上的三个点P，k_1P以及k_2P，计算k_1k_2P是困难的。

根据国际标准技术研究机构（National Institute of Standards Technology，NIST）定义，为达到与高级加密标准（Advanced Encryption Standard，AES）128比特相同的安全强度，椭圆曲线的密钥长度至少是256比特，而RSA的密钥长度至少是3072比特[47, 48]。因此，在相同等级的安全强度下，椭圆曲线的密钥和参数长度远小于RSA的密钥长度，且椭圆曲线参数规模随强度增加的增长速率也远小于RSA的增长速率。此外，大量实验结果显示[24, 25]，椭圆曲线密码学运算操作的计算开销远小于RSA操作的计算开销。

由于椭圆曲线密码学具有安全性高、密钥长度短、存储空间小、通信负荷低以及计算效率高等优势，近年来受到密码学研究者们的广泛关注，并在理论和技术上取得了大量的研究成果。本论文主要采用椭圆曲线上的无证书公钥密码学技术以及签密技术。

（1）无证书公钥密码学技术

一般来说，公钥密码学技术可以分为三类：基于证书的、基于身份的和基于无证书的[49]。无证书数字签名的概念最早由AlRiyami等人于2003年提出[50]。在无证书公钥密码学技术中，密钥生成中心（Key Generation Center，KGC）为用户生成部分私钥/公钥，用户将来自KGC的部分私钥/公钥与自身持有的部分私钥/公钥相结合，进一步获得完整的私钥/公钥。通过此种方式，即使KGC被攻陷，用户终端的完整密钥也不会暴露给攻击者，因此无证书公钥密码学技术可以解决基于身份的密码学技术中的私钥分发以及密钥托管问题。由于无证书公钥密码学技术中无需使用证书，可以避免基于证书的密码学技术中的证书管理问题。此外，相比于基于证书的密码学方案，椭圆曲线上的无证书公钥密码学方案耗费较少的通信开销和存储开销。近年来，学术界针对不同应用场景已经提出了大量的基于椭圆曲线的无证书数字签名方案[51–55]。

（2）签密技术

签密技术不仅可以同时实现加密和数字签名，而且相比于传统的“先签名后加密技术”耗费更少的计算开销和通信开销[56]。在签密技术中，发送者使用目标公钥对隐私消息进行加密，同时使用自己的私钥对消息进行签名。因此，只有目标接收者可以读取隐私消息，并且目标接收者可以使用发送者的公钥来验证签名以进一步确保数据的完整性和发送者的真实性。由于数字签名的存在，发送者不能否认他已经发送过该消息。因此，签密方案可以实现数据的机密性、完整性、真实性和不可否认性。第一个签密方案最早由Zheng等人于1997年提出[57]。目前，学术界针对不同

的应用场景已经提出了大量的签密方案[58–62]。

（3）聚合签名技术

聚合签名是一类具有聚合性质的数字签名。聚合签名具体描述如下：首先，每个用户i获得其公私钥；然后，每个用户i利用其私钥签名消息M_i输出签名δ_i。随后，输入n个用户的签名$(\delta_i)_{i=1,...,n}$以及身份信息等内容输出聚合签名δ；最后，直接通过检查聚合签名δ的有效性认证这n个用户。显而易见，采用聚合签名机制可以有效降低通信开销和计算开销。聚合签名的概念最早是由Boneh等人于2003年提出[63]。目前，学术界已经提出了大量的聚合签名相关方案[64–66]。

2.1.2　格理论密码学概述

格是线性空间上的离散加法子群，R^m上的n维格是由n个线性无关的向量组成。基于矩阵$\boldsymbol{B} = \{\boldsymbol{b_1}, \boldsymbol{b_2}, ..., \boldsymbol{b_n}\}$ 上的n维格表示为：

$$\Lambda = \mathcal{L}(\boldsymbol{B}) = \{\boldsymbol{Bc} = \sum_{i=1}^{n} \boldsymbol{c_i} \cdot \boldsymbol{b_i} : \boldsymbol{c} \in Z^n\},$$

其中，$\boldsymbol{b_1}, \boldsymbol{b_2}, ..., \boldsymbol{b_n}$代表$n$个线性无关的向量，也称为格$\Lambda$的基，且$n$为格$\Lambda$的维数，$m$为格$\Lambda$的秩。当$n = m$时，称$\Lambda$为满秩格。密码学领域大多采用的都是满秩格。

对于基于格的密码系统，安全性基于最坏情况的复杂性。格问题的主要形式就是寻找满足最小化特征的格向量。格理论密码学的安全性主要基于如下两个经典困难问题[67]。

（1） 最短矢量问题：给定格Λ的一个基$\boldsymbol{B}$，找出格Λ中的最短矢量。

（2） 最近矢量问题：给定格Λ的一个基$\boldsymbol{B}$和一个矢量t，找出格Λ上与矢量t最近的矢量。

最短矢量问题和最近矢量问题都是非确定多项式（Non-deterministic Polynomial，NP）问题。目前，绝大多数传统的公钥密码系统都是基于平均情况复杂性的，而格密码系统是基于最坏情况复杂性的。但是，一般地，基于格密码学的密钥、参数长度都很大，因此，效率还需进一步改进。

近年来量子计算机发展迅速。基于量子计算的最新发展，一些科学家甚至声称，在20年内，目前广泛使用的基于数论的公钥基础设施问题（如大整数分解问题），由于大规模量子计算机的广泛部署而变得不再安全。此外，一些国际标准组织，例如NIST指出，现在必须开始准备新的信息安全系统，使其能够抵抗量子计算，因为要确保从目前广泛使用的密码系统平稳、安全地迁移到可抵抗量子计算的对应系统，

需要付出巨大的努力[43]。因此，寻找能抵御量子计算的密码系统成为当前异常紧迫的问题。而基于格的密码系统是针对抗量子攻击的一个非常有竞争力的候选方案，其意义和作用不言而喻。本论文主要采用了格理论密码学中q元格上的困难问题，相关介绍如下。

不失一般性，整数用Z表示，向量用粗体小写字母表示，例如$\boldsymbol{e}$，而此向量的第j个元素表示为e_j，矩阵用粗体大写字母表示，例如$\boldsymbol{A}$，以及该矩阵的转置表示为$\boldsymbol{A}^t$。此外，采用$poly(n)$表示一个非指定的函数$f(n) = O(n^c)$，其中c为常量，而$w(f(n))$ 表示一组对任意$c > 0$增长速度都快于$cf(n)$的函数。读者可参阅文献[68–74]了解更多详细信息。

(1) 定义

本论文中采用的q元格的相关定义如下。

- 定义1. 对于某些正整数n，m以及q，矩阵$\boldsymbol{A} \in Z_q^{n\times m}$，$m$维$q$元格定义如下：$\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in Z^m : \boldsymbol{A}\boldsymbol{e} \equiv 0 \, mod \, q\}$[68, 69]。

- 定义2. 对任意$c \in Z_q^m$以及高斯参数σ，m维格Λ 上的离散高斯分布定义如下：$\forall \boldsymbol{x} \in \Lambda, D_{\Lambda,\sigma,c}(\boldsymbol{x}) = \rho_{\sigma,c}(\boldsymbol{x})/\rho_{\sigma,c}(\Lambda)$，其中$\rho_{\sigma,c}(\boldsymbol{x})$ 为Z^m 域上以c为中心的高斯函数。

- 定义3. 小整数解问题$SIS_{q,m,\beta}$定义为：给定素数q，一个矩阵$\boldsymbol{A} \in Z_q^{n\times m}$以及一个实数$\beta$，找到一个非零整数向量$\boldsymbol{e} \in Z^m$，满足$\boldsymbol{A}\boldsymbol{e} \equiv 0 \, mod \, q$和$\| \boldsymbol{e} \| \leq \beta$[70, 72]。

- 定义4. 非齐次小整数解问题$ISIS_{q,m,\beta}$定义为：给定q，一个矩阵$\boldsymbol{A} \in Z_q^{n\times m}$，一个实数$\beta$以及一个向量$\boldsymbol{u} \in Z_q^m$，找到一个非零整数向量$\boldsymbol{e} \in Z^m$，满足$\boldsymbol{A}\boldsymbol{e} \equiv \boldsymbol{u} \, mod \, q$和$\| \boldsymbol{e} \| \leq \beta$[68, 69]。

(2) 算法

本论文中使用到的一些概率多项式时间算法描述如下。

- $TrapSamp(1^n, q, m)$: 输入一个安全的系统参数n，一个正整数q以及一个$poly(n)$有界的正整数$m \geq 8n \, log \, q$, 输出$(\boldsymbol{A}, \boldsymbol{T})$，其中$\boldsymbol{A} \in Z_q^{n\times m}$，$\boldsymbol{T} \in Z_q^{m\times m}$的行构成了$\Lambda_q^{\perp}(\boldsymbol{A})$的一组基，并且$\| \boldsymbol{T} \| \leq O(n \, logq)$[72]。

- $ExtBasis(\boldsymbol{A}, \boldsymbol{A}', \boldsymbol{T})$: 输入两个矩阵$\boldsymbol{A} \in Z_q^{n\times m}$, $\boldsymbol{A}' \in Z_q^{n\times m'}$ 以及$\Lambda_q^{\perp}(\boldsymbol{A})$的基$\boldsymbol{T} \in Z_q^{m\times m}$，输出格$\Lambda_q^{\perp}(\boldsymbol{A} \parallel \boldsymbol{A}')$的一组基$\boldsymbol{T}' \in Z_q^{(m+m')\times(m+m')}$，其中$m'$是一个任意的正整数[73]。

- $RandBasis(\boldsymbol{T}, \sigma)$: 输入格$\Lambda_q^{\perp}(\boldsymbol{A})$的一组基$\boldsymbol{T} \in Z_q^{m\times m}$ 以及相应的高斯参数σ，输出格$\Lambda_q^{\perp}(\boldsymbol{A})$的一组新的基$\boldsymbol{T}'$[73]。

- $SamplePre(\boldsymbol{T}, \boldsymbol{u}, \sigma)$: 输入格$\Lambda_q^{\perp}(\boldsymbol{A})$的一组基$\boldsymbol{T} \in Z_q^{m \times m}$，一个参数$\boldsymbol{u} \in Z_q^n$以及相应的高斯参数$\sigma$，输出$\boldsymbol{e} \in Z_q^m$，满足$\boldsymbol{Ae} \equiv \boldsymbol{u}\, mod q$以及$\| \boldsymbol{e} \| \leq \sigma\sqrt{m}$[68]。

- $SampleDom(A, \sigma)$: 输入一个矩阵$\boldsymbol{A} \in Z_q^{n \times m}$和一个安全的高斯参数$\sigma$，输出$\boldsymbol{x} \in Z_q^m$，满足$\| \boldsymbol{x} \| \leq \sigma\sqrt{m}$，且$\boldsymbol{x}$与$SamplePre$的输出同分布[68]。

(3) Gentry加密机制[71, 72]

本论文中采用的Gentry加密机制主要包括以下几个方面。

- KeyGen: 给定一个安全参数n，一个$poly(n)$有界的正整数$m \geq 8nlogq$以及一个奇素数$q = poly(n)$，运行算法$TrapSamp(1^n, q, m)$，输出一个矩阵$\boldsymbol{A} \in Z_q^{n \times m}$作为公钥，一个基$\boldsymbol{T} \in Z_q^{m \times m}$作为私钥。

- Encryption: 随机选择一个矩阵$\boldsymbol{S_i} \in Z_q^{n \times m}$以及一个噪声矩阵$\boldsymbol{X_i} \in Z_q^{m \times m}$，采用等式$\boldsymbol{C_i} \equiv \boldsymbol{A}^t\, \boldsymbol{S_i} + 2\boldsymbol{X_i} + \boldsymbol{M_i}\, mod\, q$ 加密消息$\boldsymbol{M_i} \in Z_2^{m \times m}$。

- Decryption: 采用等式$\boldsymbol{M_i} \equiv (\boldsymbol{T}^t)^{-1}(\boldsymbol{T}^t\boldsymbol{C_i}\ \ mod\, q)\, mod\, 2$解密获得消息$\boldsymbol{M_i}$。

2.2　安全协议分析方法

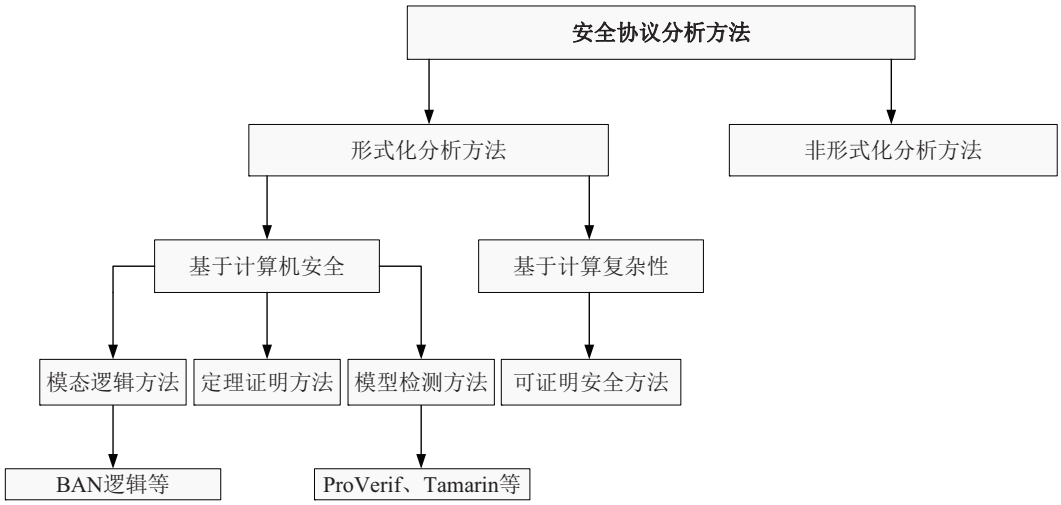


图 2.1　安全协议分析方法

安全协议分析方法是辅助协议设计，挖掘协议安全漏洞的有效手段。如图2.1所示，目前安全协议分析方法主要分为两大类，形式化安全协议分析方法和非形式化安全协议分析方法。最早出现的非形式化安全协议分析方法是指研究者采用主观经验查找协议漏洞，根据已知的各种协议攻击方法对协议进行分析和论证。形式化安全协议分析方法可以找出非形式化安全协议分析方法中无法觉察的安全漏洞。目

前，形式化安全协议分析方法主要分为两大类：基于计算机安全的分析方法和基于计算复杂性的分析方法[75]。基于计算机安全的分析方法又包括三种类型：基于知识和信念推理的模态逻辑方法，基于定理的证明方法和模型检测方法[76, 77]。最经典的模态逻辑方法是由M.Burrows、M.Abadi和R.Needham在1989年提出的BAN逻辑[78]。BAN逻辑从协议执行者最初的一些初始假设开始，根据每个诚实参与者在协议执行过程中发出、接收的消息，通过形式化的公理和逻辑推理推出最终结果。BAN逻辑的出现使得协议安全分析进入了新的阶段，改变了以往的只能凭主观经验查找协议漏洞的方法。但是，BAN逻辑分析的结果很大程度上依赖于初始假设，极大增加了协议分析结果的不准确性。

定理证明方法通过将安全协议描述为公理系统，将协议的安全属性刻画为需要证明的定理，通过公理系统中目标定理是否成立结果可以判定安全协议是否符合安全目标。定理证明方法结果相对准确，但是证明过程较为复杂，普适性不强。模型检测方法是基于硬件工作过程的模拟，将协议流程以及安全目标采用特定的形式化语言建模，并采用验证工具自动验证协议的安全目标。模型检测方法能够自动给出协议验证结果，如果不满足协议安全需求，验证工具能给出反例，以便设计者找出协议安全漏洞进而修改协议。目前，主流的模型检测工具包括AVISPA、ProVerif、Scyther以及Tamarin等[77, 79]。AVISPA不仅可以发现协议攻击和漏洞，还可以对有限和无限数量会话的协议进行验证。ProVerif可以基于一些规则推断事件是否会发生，用以实现协议机密性的验证。Scyther对于无限会话以及无限状态集合的协议可以给出明确的终止，并且支持多协议的并行分析。Tamarin可以建立无限验证、可变全局状态、归纳和循环引用。目前，AVISPA工具近年来已经停止更新，而ProVerif、Scyther以及Tamarin在过去的几年里仍然有较多扩展。此外，ProVerif和AVISPA的运行效率都较高，Scyther和Tamarin的运行效率相对而言较低[77]，但是，相比于其他工具，Tamarin工具内置较多的密码学运算包括加解密运算、结合律运算、Diffie-Hellman幂指数运算以及双线性对映射运算等[77]，进而对协议的建模更加准确。

计算机复杂性方法又称为可证明安全方法，是一种“归约”方法，通过确定协议的安全目标，构建攻击模型，将协议的安全目标归纳到密码学的一些困难问题的求解，进而证明协议的安全目标[80]。在可证明安全方法中，敌手是一个多项式时间计算的概率图灵机，但是协议的分析与论证往往需要找到一种特殊的证明途径，需要手工证明，细节问题易出错，在一定程度上限制了其广泛使用[81]。

综上所述，现有的安全协议分析方法各有其优缺点且各种安全协议分析的侧重点也各不相同。因此，在安全分析的过程中，需结合协议具体内容以及其安全目标，选择多种类型的安全协议分析方法的通用组合方式以此全方位证明协议的安全性。

在本文中，针对第一个方案，由于自动化验证工具Proverif运行效率较高，采用了ProVerif、BAN逻辑以及非形式化安全分析多维度证明了方案的安全性。针对第二个方案，由于自动化验证工具Tamarin内置的双线性映射算法支持椭圆曲线点乘操作，采用Tamarin和非形式化安全分析来证明提出方案的安全性。针对第三个方案，由于自动化验证工具在格理论领域应用较少，采用格上应用较多的可证明安全分析、BAN逻辑以及非形式化安全分析充分证明了提出方案的安全性。逻辑分析工具BAN以及自动化验证工具ProVerif和Tamarin的详细介绍如下。

2.2.1　逻辑分析工具：BAN

BAN是一种逻辑分析工具，它以知识和信仰为基础，从协议执行者最初的一些基本信仰开始，根据每个诚实参与者在协议执行过程中发出、接收的消息，通过形式化的公理和逻辑推理推出最终信仰[82]。具体的，BAN逻辑分析步骤主要包括以下几个方面。首先，对协议消息进行形式化表述。其次，定义初始假设。然后，给出协议需达到的安全目标。最后，通过消息、初始假设以及逻辑推理规则证明协议是否能够达到安全目标。如果能够达到安全目标，则验证成功；反之，验证失败。近年来，已有大量文献[83–87]采用BAN逻辑成功分析了协议的逻辑正确性。

表 2.1　BAN逻辑语法定义

符号	定义
K	共享密钥
K/K^{-1}	公钥、私钥
$P \mid\equiv X$	主体P相信X
$P \lhd X$	主体P接收到X
$P \mid\sim X$	主体P曾经发送过X
$P \mid\Rightarrow X$	主体P对X有仲裁权
$\sharp(X)$	X是新鲜的随机数
$P \overset{K}{\longleftrightarrow} Q$	主体P与主体Q共享密钥K
$\overset{K}{\longrightarrow} P$	主体P的公钥是K
$\{X\}_K$	用密钥K加密X后得到的密文
$< X >_Y$	由X和Y合成得到的消息

BAN逻辑的语法构建如表2.1所示。BAN逻辑规则描述如下[46, 88]。

1. 消息含义规则：

(1) $\dfrac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$

(2) $\dfrac{P|\equiv \xrightarrow{K} Q, P\triangleleft\{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$

(3) $\dfrac{P|\equiv P \xleftrightarrow{Y} Q, P\triangleleft\{X\}_{Y}}{P|\equiv Q|\sim X}$

2. 仲裁规则：$\dfrac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$

3. 临时值校验规则：$\dfrac{P|\equiv \sharp(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

4. 接收消息规则：

(1) $\dfrac{P\triangleleft(X,Y)}{P\triangleleft X}$

(2) $\dfrac{P\triangleleft<X>_{Y}}{P\triangleleft X}$

(3) $\dfrac{P|\equiv P \xleftrightarrow{K} Q, P\triangleleft\{X\}_{K}}{P\triangleleft X}$

(4) $\dfrac{P|\equiv \xrightarrow{K} Q, P\triangleleft\{X\}_{K}}{P\triangleleft X}$

(5) $\dfrac{P|\equiv \xrightarrow{K} Q, P\triangleleft\{X\}_{K^{-1}}}{P\triangleleft X}$

5. 新鲜性规则：

(1) $\dfrac{P|\equiv \sharp(X)}{P|\equiv \sharp(X,Y)}$

(2) $\dfrac{P|\equiv \sharp(X)}{P|\equiv \sharp(\alpha^{X})}$

6. 信念规则：

(1) $\dfrac{P|\equiv X, P|\equiv Y}{P|\equiv (X,Y)}$

(2) $\dfrac{P|\equiv (X,Y)}{P|\equiv X}$

(3) $\dfrac{P|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv X}$

(4) $\dfrac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$

7. 密钥与秘密规则：

(1) $\dfrac{P|\equiv R \xleftrightarrow{K} R'}{P|\equiv R' \xleftrightarrow{K} R}$

(2) $\dfrac{P|\equiv Q|\equiv R \xleftrightarrow{K} R'}{P|\equiv Q|\equiv R' \xleftrightarrow{K} R}$

2.2.2　形式化验证工具：Proverif

ProVerif是一个自动分析密码协议安全性的工具，可以支持对称和非对称加密、数字签名、哈希、比特承诺、非交互式零知识证明等密码学操作[89]。ProVerif的主要目标是验证密码协议。密码协议是一种并行程序，它使用公共通信信道进行交互，以实现一些与安全相关的目标，而“Dolev-Yao”能力的攻击者可以在此信道上读取、修改、删除和注入消息[90]。ProVerif工具能够证明可达性属性、对应断言和观察等价性，以此可以用于分析保密性、身份验证等属性。在Proverif模型中，加密过程是完美的，攻击者只有在拥有密钥时才能执行加解密操作。也就是说，攻击者不能执行任何多项式时间算法，只能执行用户指定的加密原语。Proverif分析考虑了无限数量的会话和无限的消息空间，解决了状态空间爆炸问题。此外，当无法证明某个属性时，ProVerif尝试重构伪造所需属性的执行跟踪。Proverif指定了重写规则和方程式，使用重写规则或相等理论来捕获加密原语之间的关系。

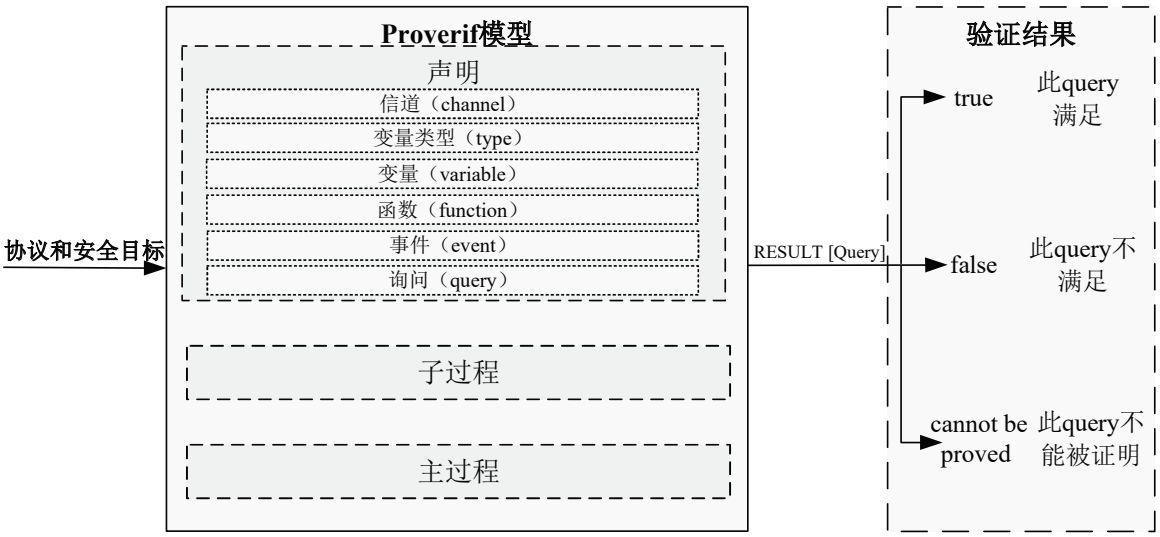


图 2.2　Proverif模型

如图2.2所示，将协议和相关的安全目标采用Proverif特定的输入语言，例如Horn子句或Pi演算建模后，Proverif验证声明的安全目标，验证完成后，自动输出验证结果[91]。协议的ProVerif模型主要包括三个部分：声明、子过程以及主过程。声明形式化了密码原语，主要包括信道$channel$、变量类型$type$、变量$variable$、函数$function$、事件$event$以及询问$query$等。Proverif支持用户自定义函数等式$function$，且采用$event$描述某个事件，而$query$则描述了协议的安全目标。子过程描述了协议中各个实体的行为，主过程则描述了协议运行的主过程，子过程和主过程均以宏定义的形式表述。Proverif工具针对每个$query$有三种不同的验证结果：$RESULT\ [Query]\ is\ true$、$RESULT\ [Query]\ is\ false$以及$RESULT\ [Query]\ cannot\ be\ proved$。$RESULT\ [Query]\ is\ true$表示此$Query$被证

表 2.2 Proverif语法定义

符号	定义
$type\ t$	类型t
$const\ n:\ t\ [data]$	公开的类型为t的全局常量n（攻击者已知t）
$const\ n:\ t\ [private]$	私有的类型为t的全局常量n（攻击者未知t）
$free\ n\ :\ t\ [data]$	公开的类型为t的全局变量n（攻击者已知t）
$free\ n\ :\ t\ [private]$	私有的类型为t的全局变量n（攻击者未知t）
$fun\ \ f(t1,...,tn)\ :\ t.$	函数f，输入为$t1,...,tn$，输出为t
$new\ n:t$	新生成类型为t的内部变量n
$if\ \ M\ \ then\ \ N\ \ else\ \ N'$	如果满足M，执行N；反之执行N'
$let\ T=M\ in\ N$	在N中令$T=M$
$out(channel,X)$	在信道$channel$上输出X
$in(channel,X)$	在信道$channel$上输入X
$event\ R$	事件R
$query\ Q$	查询条件Q是否满足
&&	与
||	或
==>	推导

明是安全的。$RESULT\ [Query]\ is\ false$表示ProVerif发现了对所查安全属性的攻击，即此$Query$被证明是不安全的。$RESULT\ [Query]\ cannot\ be\ \ proved$ 表示ProVerif无法证明此$Query$是否是安全的。Proverif中的语法定义如表2.2。近年来，已有大量的文献[92–97]采用Proverif成功分析了协议的安全性。

2.2.3 形式化验证工具：Tamarin

Tamarin也是一个可以自动分析密码协议安全性的工具[98]，可以建立无限验证、可变全局状态、归纳和循环引用，并且内置Diffie-Hellman （DH）幂指数运算、XOR运算以及双线性映射等操作。在Tamarin模型中，协议采用多集重写规则定义，属性用一阶逻辑的保护片段表示，该片段允许在时间点上进行量化[99]。Tamarin内置的敌手模型是“Dolev-Yao”。因此，在Tamarin模型中，敌手对通信网络有绝对控制权，可以窃听、删除、插入、修改和拦截公共信道上的消息。Tamarin支持两种不同的构造证明的方法：全自动模式和交互模式。在全自动模式中，如果工具的自动证明搜索终止，则返回正确性证明或反例。但是，由于安全协议的正确性可能无法判定，因此该工具可能不会在给定的验证问题上终止。因此，用户可能需要借助交互模式来探索验证状态、检查攻击图，并将手动验证指导与自动验证搜索无缝结合。

反例是所谓的依赖关系图，它是部分排序的规则实例集，表示一组违反属性的执行。反例可用于改进模型，并向实现者和设计者提供反馈。

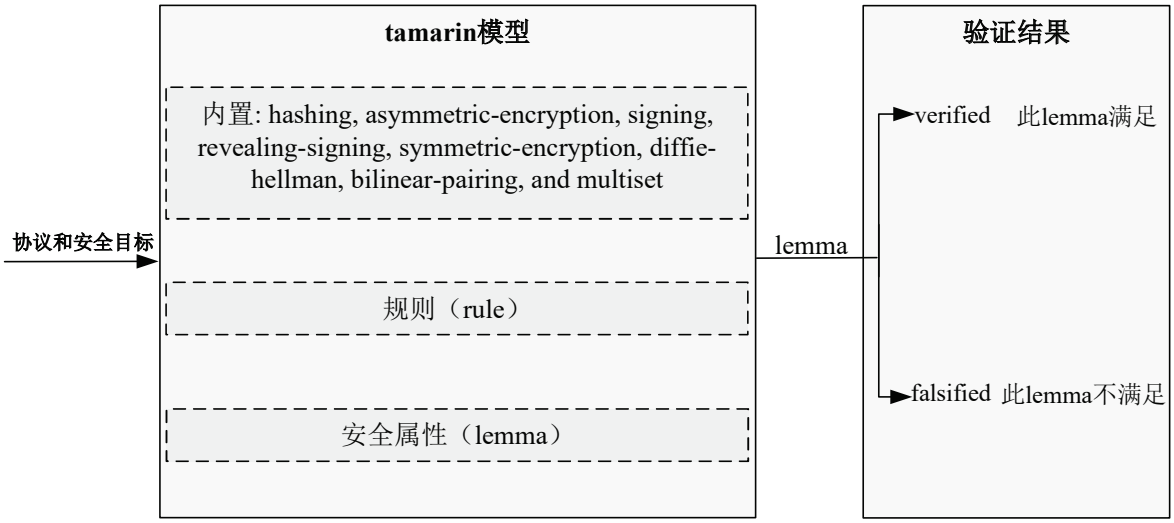


图 2.3　Tamarin模型

表 2.3　Tamarin语法定义

符号	定义
$ALL\ x$	所有x
$Ex\ y$	存在一个y
$\#\ i$	时间点i
$\$\ A$	公开的变量A
$F\ @\ \#i$	事件F发生在时间点i
$Fr(\sim t)$	新生成的变量t
$!Pk(A, pk(\sim x))$	实体A的公钥是$pk(\sim x)$
$!Ltk(A, \sim x)$	实体A的私钥是$\sim x$
$let\ T = M\ in\ N$	在N中令$T = M$
$Out(< X >)$	输出X
$In(< X >)$	输入X
$\&$	与
$\vert$	或
not	否定
$==>$	推导

如图2.3所示，将协议和相关的安全目标采用Tamarin特定的输入语言建模后，Tamarin验证声明的安全目标，验证完成后，自动输出验证结果。在Tamarin模型中，内置哈希$hashing$、非对称密钥$asymmetric-encryption$、签名$signing$、签名

验证$revealing-signing$、对称加密$symmetric-encryption$、DH 算法$Diffie-Hellman$以及双线性映射$bilinear-pairing$等多个密码学操作。重写规则$Rule$描述了协议中每个实体的具体操作，而安全属性$lemma$则描述了协议的安全目标。Tamarin中针对每个$lemma$有两种不同的验证结果：$verified$和$falsified$。$verified$表示协议满足该$lemma$。$falsified$表示验证失败，协议不满足该$lemma$。Tamarin中的语法定义如表2.3。近年来，已有大量的文献[99–104] 采用Tamarin成功分析了协议的安全性。

第三章　LTE-A网络中终端的切换认证方案

为解决LTE-A网络中多种类型基站共存导致的终端切换场景异常复杂以及现有切换认证方案存在各种各样的安全和性能漏洞等问题，本章节提出了一个适用于LTE-A网络所有移动场景的终端切换认证方案。该方案基于椭圆曲线无证书签密机制无需第三方参与即可实现终端侧与基站侧的双向认证，降低了终端切换认证复杂度，保障终端统一、安全、高效地接入LTE-A构网络。

3.1　简介

虽然3GPP已经提出了LTE-A网络终端切换认证方案[20]，但是基于S1的切换过程仍然需要终端与源基站和MME进行多轮消息交互，产生了较多的通信开销，且方案仍然存在安全或性能缺陷，例如隐私泄露、无法提供完美前向、后向安全以及前、后密钥不分离等，并不能满足当前LTE-A网络的需求。此外，学术界也提出了一些无线网络中的切换认证方案，但是存在各种安全或性能缺陷。例如，Choi等人[23]、Cao等人[24]以及Qiu等人[25]分别基于代理签名机制提出了一种切换认证方案。但是，这些方案存在一些安全漏洞，例如无法实现完美前向、后向安全、隐私保护等。因此，现有方案并不能满足当前LTE-A网络的需求，研究适用于LTE-A 网络的终端安全、高效的切换认证方案是至关重要的。

本章节，提出了一种基于无证书签密技术的隐私保护切换认证方案。在提出的方案中，利用无证书签密技术，用户终端和基站首先各自生成部分长期密钥，然后HSS分别为用户终端和基站提供另外一部分长期密钥。随后，当用户终端移动到新基站的覆盖范围时，无需第三方参与，用户终端与新基站直接使用各自的长期密钥执行切换认证与密钥协商过程。

3.2　系统模型、设计目标和设计思路

系统模型、设计目标以及设计思路如下。

3.2.1　系统模型

图3.1是LTE-A网络架构，主要包括多个MME、服务网关（Serving GateWay，S-GWs）、eNB、HeNB以及一个HSS[105]。HeNB有三种类型：封闭式HeNB、混合式HeNB和开放式HeNB。封闭式HeNB只给相应的封闭用户组（Closed Subscriber Group，CSG）成员提供服务。混合式HeNB同时给其相应的CSG 成员和非CSG成

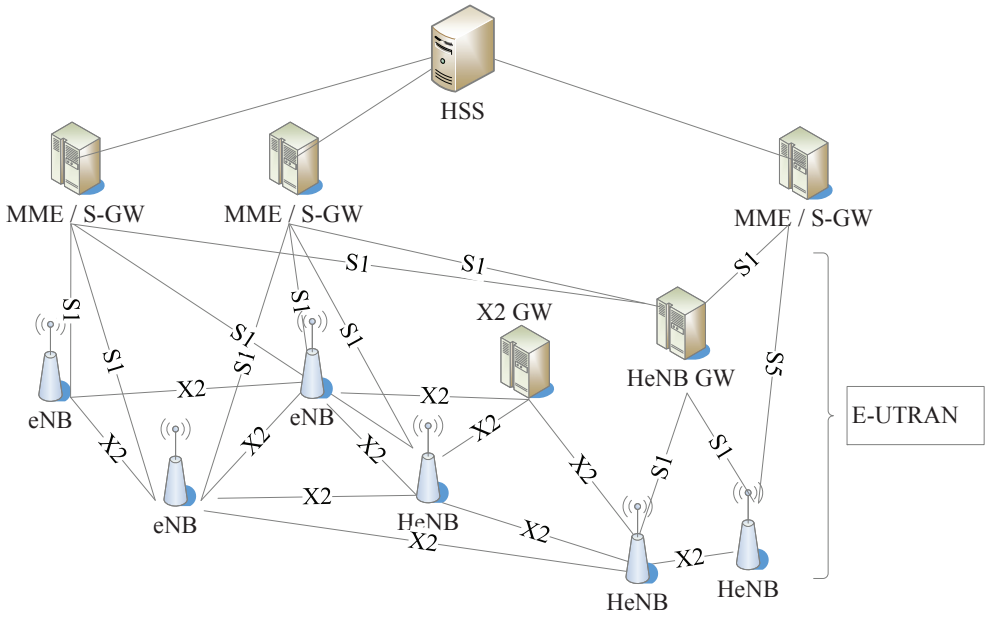


图 3.1　LTE-A网络架构

员提供服务，但不同类型的成员具有不同的优先级。开放式HeNB与普通eNB 类似[106]。3GPP委员会提出的eNB和HeNB之间的移动场景[20]主要包括以下三种类型：基于X2的切换、基于S1的切换至混合式HeNB或封闭式HeNB以及基于S1 的MME间切换。基于X2的切换是指从eNB或任意类型的HeNB切换至eNB或开放式HeNB。基于S1的切换至混合式HeNB或封闭式HeNB中，MME需要检查UE是否是目标混合/封闭式HeNB的成员。对于基于S1 的MME间切换，源基站和目标基站具有不同的MME，虽然3GPP委员会已经提出了相应的切换方案[20]，但是基于S1的切换过程仍然需要终端与源基站和MME进行多轮信息交互，产生了较多的通信开销。此外，终端在不同的移动场景需要执行不同的切换认证过程。切换认证的多样性将增加整个系统的复杂性。

3.2.2　设计目标

设计良好的LTE-A网络终端切换认证方案应该满足以下目标。

安全. LTE-A网络终端切换认证方案应该满足以下三个安全属性。

（1）相互认证与密钥协商

在切换过程中，UE与基站必须实现相互认证与密钥协商。相互认证是指UE与基站可以识别出与其通信的成员是否是合法用户。与此同时，密钥协商是指UE与基站需在切换认证过程中协商出会话密钥以保护未来通信数据的机密性。

（2）隐私保护

在切换过程中，保证用户隐私数据的机密性是至关重要的。隐私保护是指UE的

隐私数据不能公开传输，只有合法的基站才可以获取UE的隐私信息。

（3）完美前向、后向安全

在切换过程中，完美前向、后向安全也是一个重要的安全属性。完美前向、后向安全是指攻击者即使获取了UE或者基站的私钥，也无法知道之前或者之后UE与基站之间的会话密钥。

性能. LTE-A网络终端切换认证方案应该考虑以下效率需求。

（1）由于用户终端通常功率、处理能力以及存储能力受限，终端侧无法部署过于复杂的密码学算法且应尽量减少终端侧的计算开销和存储开销。

（2）由于LTE-A网络通信资源并不是非常充足，应该在满足高安全性的前提下尽量减少通信开销。

3.2.3　设计思路

本节的设计思路简要描述如下。每个合法的UE和基站在出厂使用之前会完成注册过程，预置有效的身份标识信息。当UE和基站第一次接入网络时，UE和基站分别与归属网络服务器的HSS执行初始附着过程获得完整的公私钥对。随后，当UE从源基站移动至目标基站的覆盖范围后，UE与拜访网络的目标基站直接利用各自在初始附着过程获得的完整的公私钥对执行切换认证过程。由于目标基站具有多种不同的类型，而不同类型基站中UE的移动场景也各不相同，所以将UE切换认证过程分为以下三种场景：基于X2的切换，基于S1的切换至混合式/封闭式HeNB，以及基于S1的MME 间切换。基于X2的切换适用于目标基站是普通eNB或开放式HeNB，且目标基站与源基站之间有X2连接。基于S1的切换至混合式/封闭式HeNB适用于目标基站是混合式/封闭式HeNB，且目标基站与源基站隶属于同一个MME，此时需要源MME参与完成切换认证过程。基于S1的MME间切换是指源基站与目标基站隶属于不同的MME，此时需要源MME与目标MME共同参与完成切换认证过程。切换认证过程成功完成后，UE可以通过目标基站安全地接入LTE-A网络。

3.3　方案

方案主要包括两个阶段：初始附着阶段和切换认证阶段。初始附着阶段是指当UE第一次进入网络时，UE需要与HSS进行初始认证，成功认证之后UE可以获得必要的秘密参数。而UE从一个基站移动至另外一个基站的覆盖范围时，采用初始附着阶段获得的秘密参数与目标基站执行切换认证过程。

与方案[107]中的过程类似。给定椭圆曲线E，HSS选择一个E上的循环群G，G的阶为q，生成元是P。HSS 选择一个随机数x_N作为主私钥，计算公钥$X_N = x_N P$。随后，HSS选择三个安全的单向哈希函数$H_1 : \{0,1\}^* \times G \times G \times G \rightarrow {Z_q}^*$, $H_2 : G \times$

表 3.1 符号定义

符号	定义
E/G	椭圆曲线E上的循环群G
P,q	G的生成元和阶
x_N/X_N	HSS的私钥/公钥
ID_{UE}	UE的身份标识
ID_{eNB}	eNB的身份标识
$(x_{UE},z_{UE})/(X_{UE},Y_{UE})$	UE的私钥/公钥
$(x_{eNB},z_{eNB})/(X_{eNB},Y_{eNB})$	eNB的私钥/公钥
$H_1()-H_3()$	$H_1:\{0,1\}^*\times G\times G\times G\rightarrow Z_q{}^*$,
	$H_2:G\times\{0,1\}^*\rightarrow Z_q{}^*$,
	$H_3:G\times G\rightarrow\{0,1\}^*$,

$\{0,1\}^*\rightarrow Z_q{}^*$, $H_3:G\times G\rightarrow\{0,1\}^*$。最后，HSS公开参数$\{G,q,P,X_N,H_1,H_2,H_3\}$。本章节中用到的符号定义在表3.1 中。

3.3.1 初始附着阶段

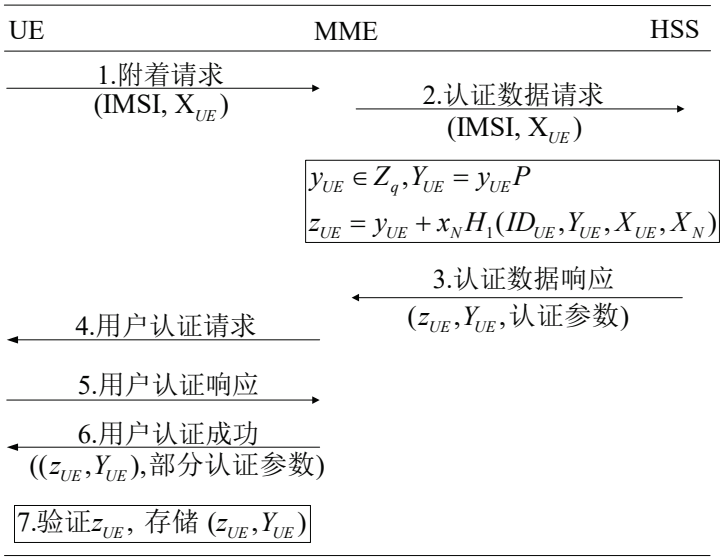


图 3.2 初始附着过程

当UE初次接入网络时，UE与网络侧实体HSS执行初始附着过程。初始附着阶段可为将来的切换认证做准备。基站和UE通过提供其有效身份和部分公私钥，可以从HSS获得另外的部分公私钥。在这里，仅介绍UE的初始附着过程。基站的初始附着过程与UE类似。图3.2呈现了UE的初始附着过程。

(1) 当UE想要注册到网络中时，他首先选择一个随机值$x_{UE}\in Z_q$并且计算$X_{UE}=$

$x_{UE}P$。随后，UE将其国际移动用户识别码（International Mobile Subscriber Identity，IMSI）以及X_{UE}包含在附着请求消息中发送给MME。

(2) MME接收到附着请求消息后，转发给HSS。

(3) HSS 选择另外一个随机值$y_{UE} \in Z_q$并且计算$Y_{UE} = y_{UE}P$。另外，HSS根据等式3-1计算UE的另外部分私钥z_{UE}。最后，HSS 将(z_{UE}, Y_{UE})以及认证参数包含在认证数据响应消息中发送给MME。

$$z_{UE} = y_{UE} + x_N H_1(ID_{UE}, Y_{UE}, X_{UE}, X_N) \tag{3-1}$$

步骤(4)、步骤(5)和EPS-AKA方案[108]中的步骤一致。

(6) MME将(z_{UE}, Y_{UE})以及部分认证参数发送给UE。

(7) UE接收到(z_{UE}, Y_{UE})后，根据等式3-2验证HSS提供的部分私钥的有效性。如果验证失败, UE发送一个认证拒绝消息给HSS。否则，UE 存储公钥(X_{UE}, Y_{UE})和私钥(x_{UE}, z_{UE})。

$$z_{UE}P = Y_{UE} + X_N H_1(ID_{UE}, Y_{UE}, X_{UE}, X_N) \tag{3-2}$$

与UE类似，合法的基站也可以生成随机数x_{eNB}作为部分私钥，计算$X_{eNB} = x_{eNB}P$作为部分公钥，并且从HSS获得另外部分私钥z_{eNB}和部分公钥Y_{eNB}。进而，基站存储(X_{eNB}, Y_{eNB})作为公钥，(x_{eNB}, z_{eNB})作为私钥。在初始附着阶段之后，每个合法的UE和基站都会获得各自完整的公钥和私钥。

根据上述初始附着过程可知，即使敌方拦截了无线通信信道，甚至MME/HSS被攻陷，UE和基站的完整私钥也不会暴露给攻击者。

3.3.2　切换认证阶段

当UE从源基站移动至目标基站的覆盖范围后，UE与目标基站利用初始附着阶段获得的公私钥对执行切换认证过程，进而，UE可以通过目标基站接入LTE-A网络。根据基站的不同类型，UE 切换认证主要分为以下三种场景：基于X2的切换，基于S1的切换至混合式/封闭式HeNB，以及基于S1的MME间切换。在本小节，采用eNB_2表示目标基站，eNB_1 表示源基站。

1. 基于X2的切换

若源基站与目标基站之间有直接的X2连接，且目标基站是开放式HeNB或普通eNB时，终端与目标基站执行基于X2的切换。如图3.3 所示，基于X2的切换主要包括以下几个步骤。

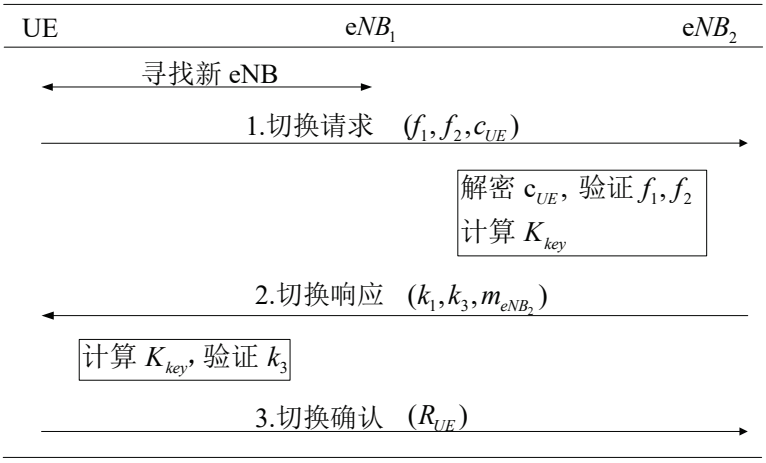


图 3.3 基于X2的切换认证过程

(1) UE在到达目标基站eNB_2的覆盖范围之前，首先从当前基站eNB_1获取eNB_2的相关信息，例如身份标识ID、公钥(X_{eNB_2}, Y_{eNB_2})以及可选的CSG 标识等。如果目标基站是混合式或者封闭式的HeNB，UE检查该基站的CSG标识在其白名单中是否存在。如果不存在，UE需要重新寻找新的目标基站。否则，UE随机选择$r \in Z_q^*$，计算f_1 和v_1。最后，UE根据等式3-3利用其私钥签名消息m_{UE}，其中m_{UE}包括用于切换认证的必要信息，例如UE的全球唯一临时终端标识（Globally Unique Temporary Identifier，GUTI），UE的公钥(X_{UE}, Y_{UE})以及当前MME的身份标识。如果目标基站是混合式/封闭式HeNB，可选的用户CSG信息也需包含在m_{UE}中。

$$\begin{aligned} f_1 &= rP \\ v_1 &= rX_{eNB_2} \\ f_3 &= H_2(f_1, m_{UE}) + H_2(v_1, ID_{eNB_2}) \\ f_2 &= r/(x_{UE} + z_{UE} + f_3) \end{aligned} \tag{3-3}$$

随后，UE根据等式3-4，采用eNB_2的部分公钥Y_{eNB_2}以及HSS的公钥X_N计算v_2，并且加密消息m_{UE}。通过此种方式，只有指定的eNB_2才可以解密密文获得正确的明文m_{UE}。

$$\begin{aligned} h_{eNB_2} &= H_1(ID_{eNB_2}, X_{eNB_2}, Y_{eNB_2}, X_N) \\ v_2 &= r(Y_{eNB_2} + h_{eNB_2} X_N) \\ c_{UE} &= H_3(v_1, v_2) \oplus m_{UE} \end{aligned} \tag{3-4}$$

最后，UE将(f_1, f_2)作为签名，c_{UE} 作为密文发送给eNB_2。

(2) eNB_2接收到消息之后，首先利用其私钥计算v_1'和v_2'，解密获得m_{UE}'。然后，

eNB_2 计算出f_3'。

$$\begin{aligned} v_1' &= f_1 x_{eNB_2} \\ v_2' &= f_1 z_{eNB_2} \\ m_{UE}' &= H_3(v_1', v_2') \oplus c_{UE} \end{aligned} \tag{3-5}$$

$$f_3' = H_2(f_1, m_{UE}') + H_2(v_1', ID_{eNB_2}) \tag{3-6}$$

最后，根据等式3-7，eNB_2利用UE的公钥(X_{UE}, Y_{UE})验证签名(f_1, f_2)，其中ID_{UE}'，(X_{UE}, Y_{UE})是从隐私消息m_{UE}'中解析得出。如果验证失败，eNB_2 给UE发送一个切换失败响应消息。否则，eNB_2成功认证UE。

$$\begin{aligned} h_{UE}' &= H_1(ID_{UE}', X_{UE}, Y_{UE}, X_N) \\ f_1 &= f_2(X_{UE} + Y_{UE} + h_{UE}' X_N + f_3' P) \end{aligned} \tag{3-7}$$

(3) 随后，eNB_2 随机选择一个数$s \in Z_q^*$，按照下列等式计算会话密钥K_{key}。

$$K_{key} = s f_1 \tag{3-8}$$

另外，eNB_2 按照如下等式计算k_1和k_3，其中m_{eNB_2}包含基站的必要信息，例如新MME的身份标识等。

$$\begin{aligned} k_1 &= sP \\ k_3 &= H_2(k_1, m_{UE}') + H_2(K_{key}, m_{eNB_2}) \end{aligned} \tag{3-9}$$

最后，eNB_2 将(k_1, k_3, m_{eNB_2})包含在切换响应消息中发送给UE。

(4) 接收到切换响应消息后，UE首先按照等式3-10计算会话密钥K_{key}。如果计算过程中没有错误，此会话密钥K_{key} 应该与eNB_2在等式3-8 中计算得出的会话密钥相同。

$$K_{key} = r k_1 \tag{3-10}$$

然后，UE按照等式3-11计算出k_3'，检查接收到的k_3是否等于k_3'。明显可知，当前只当UE与eNB_2协商的会话密钥K_{key}相同时，等式才会成立。另外，只有指定的eNB_2才可以获得m_{UE}进而产生有效的k_3。因此，如果相等，UE成功认证eNB_2。

$$k_3' = H_2(k_1, m_{UE}) + H_2(K_{key}, m_{eNB_2}) \tag{3-11}$$

(5) 为了确认会话密钥的正确性，UE发送R_{UE}给eNB_2。

$$R_{UE} = H_2(K_{key}, m_{UE}) \tag{3-12}$$

(6) eNB_2接收到R_{UE}后，计算R_{UE}'，验证R_{UE}'是否等于R_{UE}。如果验证通过，切换认证和密钥协商过程成功完成。

$$R_{UE}' = H_2(K_{key}, m_{UE}') \tag{3-13}$$

(7) 最后，eNB_2给源MME发送一个路径切换请求消息。

2. 基于S1的切换至混合式/封闭式HeNB

若源基站与目前基站隶属于同一个MME，且目标基站是混合式HeNB或封闭式HeNB时，UE与目标基站需执行基于S1的切换至混合式/封闭式HeNB认证过程。在此切换认证过程中，由于UE与目标基站之间的步骤与基于X2的切换步骤相同，这里只介绍额外的步骤。

步骤(1)和(2)与基于X2的切换中步骤(1)和(2)相同。

(3) eNB_2成功认证UE之后，将m_{UE}包含在切换请求消息中发送给MME。如果eNB_2是封闭式HeNB，切换请求消息需包含CSG标识。如果eNB_2是混合式HeNB，CSG标识以及设置为‘hybrid’的CSG接入模式需一并包含在切换请求消息中。

(4) 一旦接收到来自eNB_2的切换请求消息，MME需检查UE的CSG信息。如果针对接收到的CSG标识没有有效的CSG信息，且CSG接入模式不是‘hybrid’，MME发送一个切换请求失败消息给eNB_2。如果CSG接入模式是‘hybrid’，指示UE是否在CSG列表中的CSG成员身份指示应包括在切换请求确认消息中。最后，MME将切换请求确认消息发送给eNB_2。

(5) 接收到切换请求确认消息后，如果eNB_2是混合HeNB，则eNB_2根据CSG成员指示来对CSG成员和非CSG成员执行差异化处理。

(6) 随后，eNB_2执行与基于X2的切换中步骤(3)-(7)相同的操作。

3. 基于S1的MME间切换

若当前基站和目标基站隶属于不同的MME时，UE与目标基站执行基于S1的MME间切换认证。在此切换认证过程中，除了上述基于X2的切换步骤外，还需执行额外的步骤。

步骤(1)和(2)与基于X2的切换过程中步骤(1)和(2)相同。

(3) eNB_2成功认证UE后，将UE的GUTI等必要信息包含在切换请求消息中发送给MME。如果eNB_2是混合式/封闭式HeNB，CSG标识和接入模式都应该包含在切换请求消息中。

(4) 目标MME接收到切换请求消息后，获取源MME的信息且发送一个文本请求消息给源MME。

(5) 源MME接收到来自目标MME的文本请求消息后，将UE的安全文本发送给目标MME。

(6) 目标MME接收到文本响应消息后，检查消息内容。如果CSG标识存在，MME执行与上述基于S1的切换至混合式/封闭式HeNB中步骤(4)相同的操作。否则，目标MME发送切换请求确认消息给eNB_2。

(7) 如果eNB_2是混合式/封闭式HeNB，需执行与上述基于S1的切换至混合/封闭HeNB中步骤(5)相同的操作。随后，执行与基于X2的切换中步骤(3)、(4)、(5)以及(6)相同的操作。

(8) 切换认证和密钥协商机制成功完成后，eNB_2发送一个切换通知消息给目标MME，然后目标MME通知源基站切换过程已经成功完成。

3.4 安全评估

本小节，采用了逻辑分析工具BAN、形式化验证工具Proverif以及非形式化安全分析证明和对比了提出方案的安全性。

3.4.1 逻辑分析工具：BAN

BAN逻辑已经被广泛用于证明相互认证和密钥协商等安全属性。本小节，采用BAN逻辑分析了提出方案的逻辑正确性。首先，介绍了方案中传输的消息以及方案的安全目标。随后，给出了基本假设。最后，基于假设和BAN逻辑规则，详细证明了提出的方案可以满足安全目标。

根据提出的方案，基于X2的切换过程中涉及的消息内容如下：

M1. $UE \rightarrow eNB_2 : (f_1, f_2, c_{UE})$

M2. $eNB_2 \rightarrow UE : (k_1, k_3, m_{eNB_2})$

M3. $UE \rightarrow eNB_2 : (R_{UE})$，其中$R_{UE} = H_2(K_{key}, m_{UE})$

提出的方案的安全目标是可以实现相互认证和密钥协商，具体在BAN模型中描述如下：

G1. $eNB_2 \mid\equiv eNB_2 \overset{K_{key}}{\longleftrightarrow} UE$

G2. $UE \mid\equiv UE \overset{K_{key}}{\longleftrightarrow} eNB_2$

G3. $eNB_2 \mid\equiv UE \mid\equiv UE \overset{K_{key}}{\longleftrightarrow} eNB_2$

G4. $UE \mid\equiv eNB_2 \mid\equiv eNB_2 \overset{K_{key}}{\longleftrightarrow} UE$

由于每个消息是由相应的实体生成，下列假设必定成立。

A1. $eNB_2 \mid\equiv UE \mid\Rightarrow (f_1, f_2, c_{UE})$

A2. $UE \mid\equiv eNB_2 \mid\Rightarrow (k_1, k_3, m_{eNB_2})$

基于假设和BAN逻辑规则[88]，提出的方案可以满足上述安全目标。具体证明过程如下。

根据消息**M1**，可以得出：

Step 1. $eNB_2 \lhd (f_1, f_2, c_{UE})$

由于随机数的使用和新鲜性规则，可以得出：

Step 2. $eNB_2 \mid\equiv \sharp(f_1, f_2, c_{UE})$

根据提出的方案，eNB_2利用UE的公钥验证签名。如果验证成功，可以得出：

Step 3. $eNB_2 \mid\equiv UE \mid\sim (f_1, f_2, c_{UE})$

根据临时值校验规则，可以得出：

Step 4. $eNB_2 \mid\equiv UE \mid\equiv (f_1, f_2, c_{UE})$

根据假设**A1**和仲裁规则，可以得出：

Step 5. $eNB_2 \mid\equiv (f_1, f_2, c_{UE})$

在提出的方案中，eNB_2计算$K_{key} = sf_1$，其中s是由eNB_2选取的随机数。另外，根据信念规则，可以得出：

Step 6. $eNB_2 \mid\equiv K_{key}$，即**G1**：$eNB_2 \mid\equiv eNB_2 \overset{K_{key}}{\longleftrightarrow} UE.$

根据消息**M2**可以得出：

Step 7. $UE \lhd (k_1, k_3, m_{eNB_2})$

由于随机数的使用和新鲜性规则，可以得出：

Step 8. $UE \mid\equiv \sharp(k_1, k_3, m_{eNB_2})$

在提出的方案中，UE通过检查哈希值的正确性认证eNB_2。如果认证成功，可以得出：

Step 9. $UE \mid\equiv eNB_2 \mid\sim (k_1, k_3, m_{eNB_2})$

根据临时值校验规则，可以得出：

Step 10. $UE \mid\equiv eNB_2 \mid\equiv (k_1, k_3, m_{eNB_2})$

根据假设**A2**和仲裁规则，可以得出：

Step 11. $UE \mid\equiv (k_1, k_3, m_{eNB_2})$

在提出的方案中，UE计算$K_{key} = rk_1$, 其中r是UE选择的随机数。另外，根据信念规则，可以得出：

Step 12. $UE \mid\equiv K_{key}$，即**G2**：UE $\mid\equiv UE \overset{K_{key}}{\longleftrightarrow} eNB_2.$

根据消息**M3**，可以得出：

Step 13. $eNB_2 \lhd R_{UE}$

根据**Step 6**和消息含义规则，可以得出：

Step 14. $eNB_2 \mid\equiv UE \mid\sim R_{UE}$

由于随机数的使用和新鲜性规则，可以得出：

Step 15. $eNB_2 \mid\equiv \sharp R_{UE}$

根据临时值校验规则，可以得出：

Step 16. $eNB_2 \mid\equiv UE \mid\equiv R_{UE}$

由于$R_{UE} = H_2(K_{key}, m_{UE})$且UE的会话密钥$K_{key}$等于$eNB_2$的会话密钥，可以得出：

Step 17. $eNB_2 \mid\equiv UE \mid\equiv K_{key}$，即**G3**：$eNB_2 \mid\equiv UE \mid\equiv UE \overset{K_{key}}{\longleftrightarrow} eNB_2$.

根据**Step 10**和信念规则，可以得出：

Step 18. $UE \mid\equiv eNB_2 \mid\equiv k_3$，其中$k_3 = H_2(k_1, m_{UE}') + H_2(K_{key}, m_{eNB_2})$

因此，可以得出：

Step 19. $UE \mid\equiv eNB_2 \mid\equiv K_{key}$，即**G4**：$UE \mid\equiv eNB_2 \mid\equiv eNB_2 \overset{K_{key}}{\longleftrightarrow} UE$.

基于上述的安全分析，4个安全目标都成功实现。因此，在提出方案的切换认证过程中，UE与eNB_2可以实现相互认证，且同时协商出相同的会话密钥。

3.4.2　形式化验证工具：Proverif

本小节，采用形式化验证工具Proverif[89, 109]证明了提出方案的安全性，包括相互认证、密钥协商和数据机密性。此处重点关注基于X2的切换认证过程且假设UE和eNB_2都已经获得了相应地公钥和私钥。详细步骤如下。

首先，UE和eNB_2之间的信道和变量的基本类型定义如下。

```
(* Channel *)
free public_channel: channel.


(*Types*)
type G.
type Z.
type rand.
```

变量具体定义如下。假设UE已经获得了eNB_2的相关信息，例如ID_{eNB}。$secrectUEMsg$和$secrecteNBMsg$用于标识未来的通信数据。

```
(* variable *)
const P: G [data].
const IDeNB: rand [data].
free secrectUEMsg,secrecteNBMsg: bitstring [private].
```

函数定义如下。

```
(* function *)
fun H2(G,rand): Z.
fun H3(G): rand.
fun addZ(Z,Z): Z.
fun addG(G,G): G.
fun mul(Z,Z): Z.
fun xor(rand,rand):rand.
reduc forall x: rand, y: rand; dxor(xor(x,y),y) = x.
fun point_mul(G, Z): G.
equation forall x:Z,y:Z;point_mul(point_mul(P,x),y)=point_mul(point_mul(P,y),x).
(* connector *)
fun con(rand,G): rand.
reduc forall x: rand, y: G; dcon1(con(x,y)) = x.
reduc forall x: rand, y: G; dcon2(con(x,y)) = y.
(* Signature verification *)
fun sign(Z,Z): Z.
reduc forall x: Z,sN: Z; checksign(sign((x),sN), point_mul(P,sN)) = x.
(* Shared key encryption *)
fun sencrypt(bitstring,G): bitstring.
reduc forall x: bitstring, y: G; sdecrypt(sencrypt(x,y),y) = x.
```

定义以下几个事件来检验认证属性。

```
(* Events *)
event termI(rand, rand,bitstring).
event acceptsI(rand,rand,G,bitstring).
event acceptsR(rand,rand,bitstring).
event termR(rand,rand,G,bitstring).
```

为了测试提出的方案是否可以满足相互认证、密钥协商和数据机密性等安全属性，在主过程中需要包含以下几个*queries*。前两个*queries*表示相互认证特性。相互认证特性是通过确保$event(acceptsR())$必须在$event(termI())$之前执行，并且$event(acceptsI())$必须在$event(termR())$之前执行。第三个$query$ 表明如果UE和eNB_2成功完成相互认证，他们会协商出相同的会话密钥。最后两个*queries*代表未来通信数据的机密性。

```
(* queries *)
query x: rand, y:rand, m: bitstring;
      inj-event(termI(x,y,m)) ==> inj-event(acceptsR(x,y,m)).
query x: rand,y:rand, k:G, m: bitstring;
      inj-event(termR(x,y,k,m)) ==> inj-event(acceptsI(x,y,k,m)).
query x: rand, y:rand, k:G, k':G, m: bitstring;
      event(termR(x,y,k,m)) && event(acceptsI(x,y,k',m)) ==> k = k'.
query attacker(secrectUEMsg).
query attacker(secrecteNBMsg).
```

UE的切换认证过程具体如下。

```
let processUE(sUE:Z,pkUE:G,pkeNB:G)=
new IDUE: rand;
(* 1.handover request *)
new r: Z;
let f1 = point_mul(P,r) in
let v1 = point_mul(pkeNB,r) in
let mUE = con(IDUE,pkUE) in
```

```
let f3 = addZ(H2(f1,mUE),H2(v1,IDeNB)) in
let f2 = sign(f3,sUE) in
let cUE = xor((mUE),H3(v1)) in
out(public_channel,(f1,f2,cUE));
(* 4.compute key and verify*)
in(public_channel,(k1x: G, k3x:Z,meNBx: rand));
let key = point_mul(k1x,r) in
if k3x =  addZ(H2(k1x,mUE),H2(key,meNBx)) then
event termI(IDUE, IDeNB, (f1,f2,cUE,k1x,k3x,meNBx));
(* 5.handover confirm *)
event acceptsI(IDUE, IDeNB, key ,(k1x,k3x,meNBx,H2(key,mUE)));
out(public_channel,H2(key,mUE));
out(public_channel,sencrypt(secrectUEMsg,key)).
```

eNB_2切换认证过程具体如下。

```
let processeNB(seNB:Z,pkeNB:G)=
new meNB: rand;
(* 2.decrypt, verify and compute key*)
in(public_channel,(f1x:G,f2x:Z,cUEx:rand));
let v1x = point_mul(f1x,seNB) in
let mUEx = dxor(cUEx,H3(v1x)) in
let IDUEx = dcon1(mUEx) in
let pkUEx = dcon2(mUEx) in
let f3x = addZ(H2(f1x,mUEx),H2(v1x,IDeNB)) in
let(=f3x) = checksign(f2x,pkUEx) in
new s: Z;
let key = point_mul(f1x,s) in
(* 3.handover response *)
let k1 = point_mul(P,s) in
let k3 = addZ(H2(k1,mUEx),H2(key,meNB)) in
event acceptsR(IDUEx, IDeNB, (f1x,f2x,cUEx,k1,k3,meNB));
out(public_channel,(k1,k3,meNB));
in(public_channel,h:Z);
if h = H2(key,mUEx) then
event termR(IDUEx, IDeNB, key, (k1,k3,meNB,h));
out(public_channel,sencrypt(secrecteNBMsg,key)).
```

主过程如下。UE的公钥和私钥分别表示为$pkUE$和sUE，基站eNB_2的公钥和私钥分别表示为$pkeNB$和$seNB$。

```
process
new sUE: Z;
let pkUE = point_mul(P,sUE) in
new seNB: Z;
let pkeNB = point_mul(P,seNB) in
((!processUE(sUE,pkUE,pkeNB))|(!processeNB(seNB,pkeNB)))
```

ProVerif执行结果如下所示。结果表明，该方案能够实现相互认证、密钥协商和数据机密性。

```
RESULT inj-event(termI(x_89,y_90,m)) ==>inj-event(acceptsR(x_89,y_90,m)) is true.
RESULT inj-event(termR(x_91,y_92,k,m_93)) ==>
inj-event(acceptsI(x_91,y_92,k,m_93)) is true.
RESULT event(termR(x_94,y_95,k_96,m_97)) &&
event(acceptsI(x_94,y_95,k',m_97)) ==> k_96 = k' is true.
RESULT not attacker(secrectUEMsg[]) is true.
RESULT not attacker(secrecteNBMsg[]) is true.
```

3.4.3 非形式化安全分析

本小节，采用非形式化安全分析证明了提出方案的安全性。

（1）相互认证

在切换认证过程中，一方面，UE使用私钥生成签名。由于私钥是不可伪造的，只有合法的用户才可以计算出有效的签名。因此，eNB_2可以通过检查签名认证UE。另外一方面，UE用eNB_2的公钥加密消息m_{UE}，只有指定的eNB_2可以解密c_{UE}获得m_{UE}，进而利用m_{UE}产生确认消息k_3。因此，UE 可以通过检查k_3认证eNB_2。因此，提出的方案可以实现相互认证。

（2）密钥协商

在切换认证过程中，UE将f_1发送给eNB_2且eNB_2发送k_1给UE。随后，UE与eNB_2采用ECDH算法协商会话密钥。因此，即使攻击者窃听了消息f_1和k_1，由于ECDHP以及ECDLP，攻击者也不可能获得会话密钥。

（3）隐私保护

在提出的方案中，由于UE的隐私信息m_{UE}采用了eNB_2的公钥进行加密，只有指定的eNB_2可以解密获得明文消息。因此，任何攻击者都不可能获得用户的隐私信息。

（4）完美前向、后向安全

在提出的方案中，UE端会话密钥的生成依赖于随机数r和公开值k_1，eNB_2端会话密钥的协商依赖于私有值s和公开值f_1。基于ECDLP，攻击者从公开值f_1中导出r或者从公开值k_1中导出s是困难的。即使攻击者获得了UE的私钥(x_{UE}, z_{UE})，由于私有值f_3的存在，攻击者也不可能获得r进而导出会话密钥。同样，即使eNB_2的私钥泄露，攻击者也不可能获得s进而导出会话密钥。因此，该方案可以提供完美前向、后向安全。

（5）抵挡多种协议攻击

提出的方案可以抵挡以下几种已知的协议攻击，包括重放攻击、中间人攻击、假冒攻击、被动攻击以及私钥泄露攻击。

① 抵抗重放攻击：由于在每个会话中均使用了新鲜的随机数，提出的方案可以抵抗重放攻击。此外，一旦目标eNB接收到切换请求消息，eNB给UE发送切换响应消息并等待确认消息。如果目标eNB没有接收到确认消息，则认为连接失败。攻击者无法通过发起重放攻击来生成确认消息，因此提出的方案能够抵抗重放攻击。

② 抵抗中间人攻击：首先，在切换认证过程中，由于UE与eNB_2完成了相互认证，任何攻击者都无法伪造UE或者eNB_2去欺骗另外一方。然后，在切换认证

完成之后，UE与eNB_2采用切换认证过程中协商的会话密钥加密数据，任何攻击者都不可能通过拦截信道公共数据获得会话密钥，进而去欺骗UE或eNB_2。因此，提出的方案可以抵抗中间人攻击。

③ 抵抗假冒攻击：这里主要考虑两种类型的假冒攻击，攻击者假冒eNB_2和攻击者假冒UE。首先，在切换认证过程中，由于攻击者不可能获得私钥(x_{eNB_2}, z_{eNB_2})，因此只有指定的eNB_2可以解密c_{UE}获得m'_{UE}，进而计算出哈希值$k_3 = H_2(k_1, m_{UE}') + H_2(K_{key}, m_{eNB_2})$且发送$k_3$给UE。随后，UE 利用其$m_{UE}$验证$k_3$的有效性。攻击者没有$m_{UE}$不可能伪造出有效的哈希值$k_3$，因此，攻击者不可能假冒$eNB_2$。此外，由于攻击者不可能得到$(x_{UE}, z_{UE})$进而产生有效的签名，因此，攻击者也不可能伪造为合法的UE。因此，提出的方案可以抵抗假冒攻击。

④ 抵抗被动攻击：在切换认证过程中，UE的隐私消息是通过目标基站的公钥加密后公开传输的，只有目标基站可以解密获得明文消息。在切换认证过程完成之后，通信数据是通过UE与eNB_2协商的会话密钥K_{key}进行加密后公开传输的。因此，在提出的方案中，攻击者不可能发起被动攻击。

⑤ 抵抗私钥泄露攻击: 如果私钥泄露，则攻击者就可以利用私钥伪造成为合法的UE或eNB_2。在提出的方案中，UE或者eNB_2的私钥来自两部分内容，一部分来自HSS，另外一部分由UE或者eNB_2自己产生。即使敌手可以窃听来自HSS的部分私钥，攻击者也不可能得到UE或者eNB_2自己产生的部分私钥。因此，提出的方案可以抵抗私钥泄露攻击。

表 3.2　安全对比

方案 / 安全属性	Qiu[25]	Cao[24]	Jing[22]	Kim[21]	Choi[23]	我们的方案
相互认证	√	√	√	√	√	√
密钥协商	√	√	√	×	√	√
隐私保护	×	×	√	√	×	√
完美前向、后向安全	√	×	×	×	×	√
避免密钥托管问题	×	×	×	×	√	√

安全对比: 如前面章节所述，相互认证、密钥协商、隐私保护以及完美前向、后向安全是切换认证过程中的重要安全属性。因此，比较了我们提出的方案与先前的方案中的重要安全属性。表3.2显示了安全属性的对比结果。具体分析如下：Cao的方案和Jing的方案都无法实现完美前向、后向安全，因为在这两个方案

中使用代理签名算法会导致用于计算会话密钥的随机数的暴露，进而攻击者能够根据随机数计算出会话密钥。在Qiu的方案和Cao的方案中，隐私信息在空口上以明文形式传输，因此这两种方案不能实现隐私保护。在Jing的方案中，由于当前基站的协助，该方案可以实现隐私保护，但是该方案并没有提及密钥协商过程。在Qiu 的方案、Cao的方案、Jing的方案和Kim 的方案中，私钥完全依赖于服务器，例如HSS。一旦UE/eNB与服务器之间的通信信道被攻陷，攻击者可以很容易地获得所有UE/eNB的私钥，因此这些方案无法避免密钥托管问题。利用无证书公钥密码技术，我们提出的方案可以避免密钥托管问题。此外，利用签密技术构造了一种新的安全切换认证方法，在不牺牲安全性的前提下进行了一些修改，以适应LTE-A网络的多种移动切换场景。利用签密技术，我们提出的方案可以实现相互认证、隐私保护等安全特性。此外，由于UE同时使用其私钥和目标基站的公钥对消息进行签名，即使敌方获得UE的私钥，也无法从签名算法中获得用于计算会话密钥的随机数。因此，我们的方案可以实现完美前向、后向安全。

3.5 性能分析

通信开销、计算开销和存储开销被认为是切换认证过程中最重要的性能指标。在本小节，对比了我们的方案与其他几种类似方案的通信开销、计算开销以及存储开销。对比方案包括Cao的方案[24]、Jing的方案[22]、Qiu的方案[25]、Choi的方案[23]以及Kim的方案[21]。为了达到与AES 128比特相同的安全级别，假设基于椭圆曲线密码学算法的密钥大小为256比特，基于RSA大整数分解算法的密钥大小为3072比特，基于有限域密码学算法公钥的大小是3072比特，私钥的大小是256比特[47]。此外，哈希函数的输出长度为128比特，随机数的大小为128比特，时间戳的大小为32比特[48]。由于所有现有的方案都需要传输诸如身份信息之类的必要信息，因此假设必要信息的长度为320 比特。

3.5.1 通信开销

表 3.3 通信开销

方案 / 消息(字节)	Qiu[25]	Cao[24]	Jing[22]	Kim[21]	Choi[23]	我们的方案
Msg1	304	856	460	104	808	264
Msg2	304	872	84	96	824	136
Msg3	16	16	16	16	16	32
总消息	624	1744	560	216	1648	432

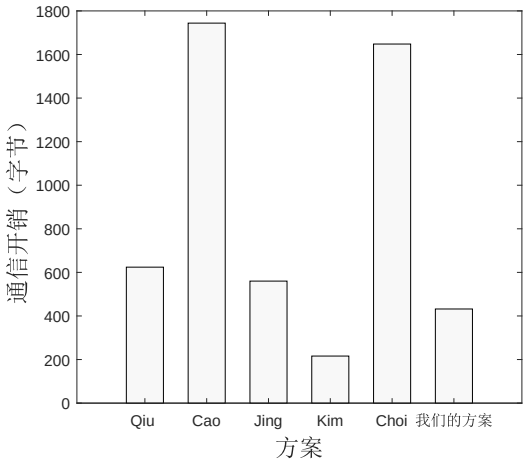


图 3.4　通信开销对比

在切换认证过程中，除了Jing的方案，其他方案中UE和目标基站之间需要交换三条消息：Msg1、Msg2以及Msg3，并且这些方案中均无需源基站的参与。为了公平起见，假设Jing的方案中，Msg1 的通信开销还包括UE与源基站eNB之间的通信开销。因此，可以通过计算消息的总大小来分析和对比现有方案的通信开销。表3.3列出了所有对比方案的通信开销。图3.4显示了我们方案与其他方案的总的通信开销对比结果。根据图3.4可知我们方案的通信开销稍大于Kim的方案，而远小于其他方案。原因主要包括以下几个方面：Kim的方案在切换认证过程中主要传输了2个椭圆曲线上的点以及一些对称密文，所以耗费的通信开销最少；Cao的方案和Choi方案在切换认证过程中主要传输了多个有限域密码学算法的公钥，所以耗费的通信开销最多；Qiu的方案在切换认证过程中主要传输了6个椭圆曲线上的点以及其他参数；我们的方案传输了4个椭圆曲线上的点以及其他较小的参数，所以我们方案的通信开销大于Kim的方案且小于其他方案，但是Kim的方案由于采用了双线性映射操作会耗费大量的计算开销。

3.5.2　存储开销

表 3.4　存储开销

方案(字节)	Qiu[25]	Cao[24]	Jing[22]	Kim[21]	Choi[23]	我们的方案
存储开销	296	1616	328	224	1664	288

在存储开销方面，由于UE的存储资源通常是受限的，因此只考虑UE端的存储需求。对于Qiu的方案，UE需要存储代理签名信息和公共参数。对于Cao的方案，UE需要存储长期密钥和公共参数。对于Jing 的方案，UE需要存储代理委托信息和公共参数。对于Kim的方案，UE需要存储其私钥和公共参数。对于Choi的方案，UE需要存

储密钥、证书和公共参数。对于我们提出的方案，UE需存储其私钥、部分公钥和公共参数。表3.4列出了现有方案的存储开销。图3.5给出了现有方案存储开销的对比结果。

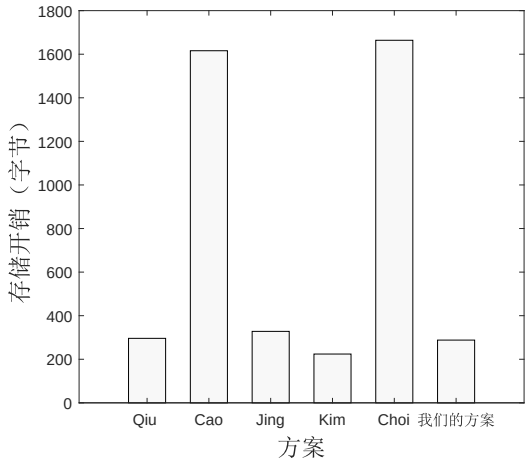


图 3.5 存储开销对比

根据图3.5可知，我们方案中UE的存储开销大于Kim方案中UE的存储开销，但是小于其他方案中UE的存储开销。Kim的方案由于只需存储基于身份公钥密码学技术中的公钥相关信息，所以存储开销较少，但是基于身份公钥密码学技术中采用了双线性映射操作，Kim的方案会产生大量的计算开销。Qiu的方案、Jing的方案以及我们提出的方案都是基于椭圆曲线上的离散对数问题，所以存储开销相近。Cao的方案和Choi的方案都是基于有限域上的离散对数问题，所以需存储有限域上公钥相关参数，存储开销较大。

3.5.3 计算开销

表 3.5 部分密码学操作的计算时间

操作(毫秒)	符号	UE	eNB
模指数	T_E	1.893	0.997
点乘	T_M	0.960	0.366
双线性映射	T_P	16.526	5.699
RSA验证	T_{RV}	1.039	0.566

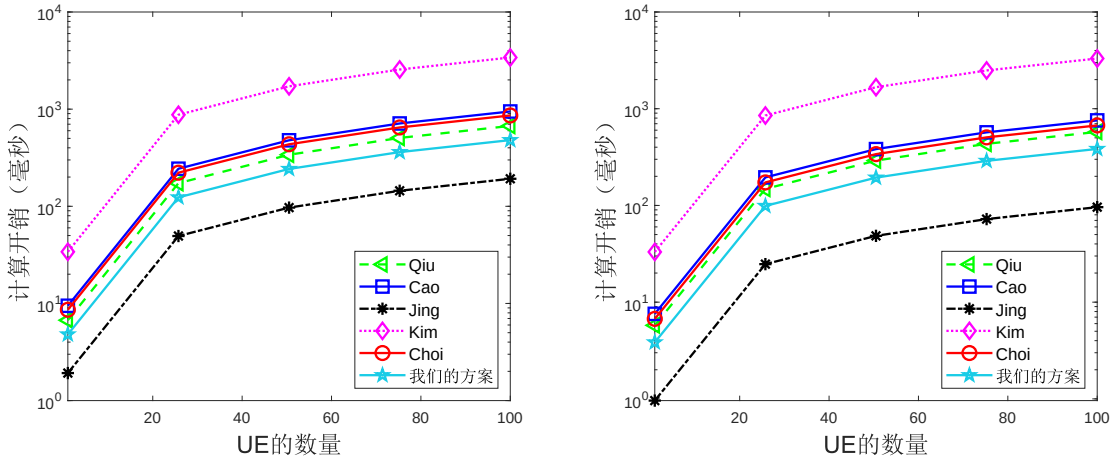
借助于C/C++OPENSSL库[110]，分别采用Intel(R) Core(TM) m3-6Y30 CPU 0.9GHz处理器作为UE和Intel(R) Core(TM) i5-7500 CPU 3.40GHz处理器作为基站测试了对比论文中主要密码学操作的计算时间。另外，采用了Barreto-Naehrig曲线测试了双线性映射的计算时间[111]。由于在这些方案中，模指数操作、椭圆曲线点乘操作、双线性映

表 3.6　无预先计算的计算开销

方案(毫秒)	T_{UE}	T_{eNB}	T_{tot}
Qiu[25]	$7T_M = 6.720$	$8T_M = 2.928$	9.648
Cao[24]	$5T_E = 9.465$	$5T_E = 4.985$	14.450
Jing[22]	$2T_M = 1.920$	$6T_M = 2.196$	4.116
Kim[21]	$T_M + 2T_P = 34.012$	$T_M + 2T_P = 11.764$	45.776
Choi[23]	$4T_E + T_{RV} = 8.611$	$4T_E + T_{RV} = 4.554$	13.165
我们的方案	$5T_M = 4.800$	$7T_M = 2.562$	7.362

表 3.7　有预先计算的计算开销

方案(毫秒)	${T_{UE}}^{pre}$	${T_{eNB}}^{pre}$	${T_{tot}}^{pre}$
Qiu[25]	$6T_M = 5.760$	$6T_M = 2.196$	7.956
Cao[24]	$4T_E = 7.572$	$4T_E = 3.988$	11.560
Jing[22]	$1T_M = 0.960$	$5T_M = 1.830$	2.790
Kim[21]	$2T_P = 33.052$	$2T_P = 11.398$	44.450
Choi[23]	$3T_E + T_{RV} = 6.718$	$3T_E + T_{RV} = 3.557$	10.275
我们的方案	$4T_M = 3.840$	$6T_M = 2.196$	6.036



(a) 无预先计算的计算开销　　(b) 有预先计算的计算开销

图 3.6　计算开销对比

射操作和RSA 验证操作占据了主要的计算开销，因此只考虑这四种操作。测试结果如表3.5所示。

表3.6显示了所有对比方案在切换认证过程中无预先计算的计算开销分析结果，其中UE端和基站端的无预先计算的计算开销分别表示为T_{UE} 和T_{eNB}，无预先计算的总计算开销表示为T_{tot}。表3.7展示了所有对比方案在切换认证过程中有预先计算的计算开销分析结果，其中UE端和基站端的有预先计算的计算开销分别表示为${T_{UE}}^{pre}$和${T_{eNB}}^{pre}$，有预先计算的总计算开销表示为${T_{tot}}^{pre}$。

由于UE的功率和处理能力通常是受限的，这里只对比我们方案与其他方案中UE的计算开销。对比结果如图3.6所示。根据图3.6，我们方案的计算开销略大于Jing的方案，而小于其他方案。由于Jing的方案中会借助于源基站完成UE隐私信息的加密，UE侧无需再次执行加密操作，所以UE侧耗费的计算开销最少。但是，Jing的方案中，引入源基站带来了一些额外的通信开销和计算开销，且Jing的方案无法实现完美前向、后向安全等属性。

3.5.4 恶意UE下的计算开销

表 3.8 恶意UE下eNB的计算开销

方案(毫秒)	T_{eNB}
Qiu[25]	$4T_M = 1.464$
Cao[24]	$3T_e = 2.991$
Jing[22]	$4T_M = 1.464$
Kim[21]	$2T_p + 1T_M = 11.764$
Choi[23]	$3T_e + 1T_{RV} = 3.557$
我们的方案	$5T_M = 1.830$

尽管前面已经证明了我们的方案能够抵抗几种已知的协议攻击，但是可能存在一些未知或者不确定的攻击，无法找到并确定我们提出的方案是否能够抵抗这些攻击。在切换认证阶段，恶意UE 如果向目标基站发送多个恶意请求消息，目标基站需处理恶意请求消息从而耗费大量的计算开销。在此种情况下，讨论基站识别恶意UE所需的计算开销。表3.8显示了恶意UE下基站侧的计算开销，其中T_{eNB}表示基站检测恶意UE所需的计算开销。

图3.7显示了恶意UE下基站侧计算开销的对比结果。根据图3.7，我们方案中基站识别恶意UE的计算开销稍大于Qiu 的方案和Jing的方案。原因主要包括两个方面：一方面，在Qiu、Cao和Choi的方案中，隐私信息以明文方式传输，因此不需要目标基站执行解密操作获得明文信息；另外一方面，对于Jing 的方案，切换认证过程需要源基站的参与，会产生额外的通信和计算开销，且无法实现完美前向、后向安全

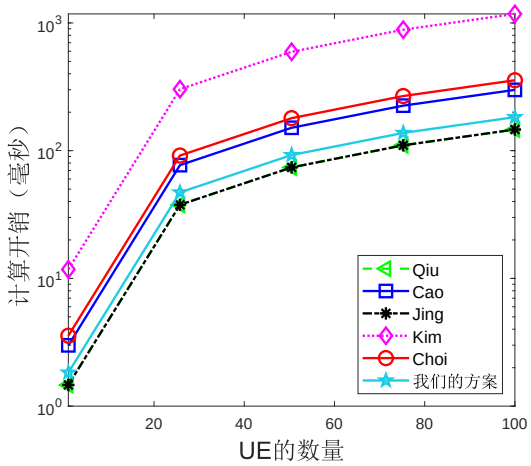


图 3.7　恶意UE下eNB的计算开销对比

等属性。

讨论: 结合上述安全性对比结果，对所提出的方案与其他相关方案进行了详细的比较。首先，与Qiu的方案相比，我们的方案不仅耗费较少的通信开销、存储开销和计算开销，而且提供隐私保护。此外，在Qiu的方案中，UE/eNB的私钥完全依赖于HSS，一旦UE、eNB和HSS之间的通信信道被破坏，UE和eNB的密钥都将暴露给攻击者。此外，若UE 和eNB 的私钥均被泄漏，则UE和eNB之间的会话密钥也将暴露给对手。因此，Qiu的方案不能完全实现完美前向、后向安全。在我们提出的方案中，由于使用了无证书公钥密码学技术，攻击者不可能获得完整的私钥并进一步获得会话密钥。其次，我们方案的通信开销、存储开销和计算开销以及恶意UE下的的计算开销均小于Cao的方案。此外，我们的方案可以提供更强的安全属性，包括完美前向、后向安全和隐私保护。随后，虽然我们方案的计算开销大于Jing的方案，但是我们方案的存储开销和通信开销远小于Jing的方案，且Jing的方案无法实现完美前向、后向安全。然后，Kim方案的计算开销远大于我们方案的计算开销，且不能实现密钥协商和完美前向、后向安全。最后，Choi的方案无法实现隐私保护和完美前向、后向安全，并且比我们的方案耗费更多的通信开销和存储开销。综上所述，我们提出的方案可以在不牺牲效率的前提下，实现更安全的切换认证过程。

3.6　结论

本章节提出了一种基于无证书签密的统一、安全的切换认证方案。该切换认证方案不仅可以应用于LTE-A网络中所有的移动切换场景，而且可以实现健全的安全属性，包括相互认证、密钥协商、隐私保护和完美前向、后向安全等。此外，安全性和性能评估结果表明，与其他方案相比，我们的方案不仅能够提供健壮的安全属

性，还具有合理的效率。

第四章　高铁网络中移动中继的群组预切换认证方案

为解决高铁网络中引入MRN导致的新的安全问题以及当前3GPP定义的MRN的切换认证机制仍然无法为用户提供平滑的通信体验等问题，本章节提出了两个群组预切换认证方案FTGPHA1 和FTGPHA2。在提出的两个方案中，MRN群组可以提前在到达目标基站覆盖范围前与目标基站执行群组预切换认证与密钥协商过程，MRN的切换认证时延可以被忽略，可以为列车上的用户终端提供较为平滑的通信体验。另外，考虑到列车在某基站逗留时间可能极短，无法完成一个切换认证过程的问题，提出的两个方案中另外考虑了协同切换认证机制，以进一步减少通信和计算开销。

4.1　简介

学术界针对MRN只提出了少量的切换认证方案[10, 11, 27–31]，但是现有方案存在各种安全和性能缺陷，例如并未实现前后密钥分离、完美前向、后向安全、匿名性等特性或耗费了较多的切换开销等。此外，文献[10, 27–29, 31]中的方案只考虑了单个MRN。随着5G高铁网络的快速发展，列车将承载越来越多的用户终端，一个单一的MRN可能无法提供高质量的网络服务。对于文献[11, 30]中的方案，列车上可以部署多个MRN以确保高质量的网络服务，且该方案利用了群组切换认证方案进一步降低了切换开销。但是在文献[11]的方案中，MRN群主首先执行切换过程，随后，普通的MRN启动切换认证过程，这无疑会增加切换认证的时延。另外，文献[11, 30]中的方案存在一些安全漏洞。

针对其他无线网络，学术界的研究者已经提出了几个群组切换认证方案[65, 112–115]。在文献[112–114]的方案中，当第一个UE执行切换过程时，源eNB将群组成员的所有安全上下文发送给目标eNB。因此，其余的组成员UE可以在没有源eNB的协助下直接执行切换过程。然而，文献[112–114]中的方案均耗费了大量的切换开销，以及并未实现一些重要的安全特性，例如隐私保护以及完美前向、后向安全等。Lai等[65]基于新颖的无证书聚合签名技术提出了一个安全有效的组漫游认证方案。在该方案中，接入网络可以同时认证所有组成员。但是，组成员却不能成功认证接入网络，因此该方案不能实现相互认证。Cao等[115]针对LTE-A网络海量机器类型通信场景提出了一个统一的组切换认证方案。由于多签名技术和聚合消息验证码的使用，该方案可以很大程度的减少信令开销，避免信令冲突。但是，该方案并未实现隐私保护以及完美前向、后向安全等安全属性，且由于多个模指数操作的使用，该方案耗费了大量的计算开

销。

综上所述，现有群组方案并不能满足5G高铁网络MRN群组切换认证需求，研究适应于高铁网络中MRN的安全、无缝的群组切换认证方案是至关重要的。

本章节，采用群组预切换认证机制，MRN在源基站的覆盖范围内提前与目标基站执行群组预切换认证过程。在群组预切换认证过程中，由于列车仍然在源基站的覆盖范围内，列车上的UE 可依赖于当前信号仍然较强的源基站完成平滑的通信，而当列车进入目标基站的覆盖范围后，MRN可直接利用预切换认证过程获得的信息与目标基站进行通信，而无需再次执行切换认证，因此可为用户终端提供较为平滑的通信体验。此外，在切换过程中，若检测到列车在下个基站逗留时间极短无法完成一次完整的切换过程，则MRN群组在源基站的覆盖范围内同时与下个基站与下下个基站提前执行群组预切换认证过程，避免MRN在下个基站逗留时间较短无法完成与下下个基站的切换过程。进而，考虑到未来5G高铁网络的异构性，在某些场景下，用户性能较差且需要较低的安全需求，而在其他场景，用户性能较强且需较强的安全属性。因此，本章节，提出了两种固定路径群组预切换认证方案（Fixed-Trajectory Group Pre-Handover Authentication scheme，FTGPHA）：方案FTGPHA1和方案FTGPHA2。在FTGPHA1，基于当前的接入认证标准5G-AKA/EAP-AKA’，提出了群组快速预切换认证过程。在FTGPHA2，每个MRN的公私钥包括两部分内容：一部分自己生成，另外一部分来自接入网络，每个MRN 利用完整的公私钥对与目标基站实现预切换认证步骤。

4.2 系统模型、设计目标和设计思路

本小节，详细描述了系统模型、设计目标以及设计思路。

4.2.1 系统模型

图4.1描述了5G高铁网络架构，主要包括四部分内容：$D-SDN$[116]、宿主基站（Donor New Radio Node B，DgNB）、MRN以及UE。$D-SDN$可以看做是一个运行在5G核心网络服务器上的软件[117]。$D-SDN$和DgNBs是通过有线网络连接，而DgNBs和MRN是通过无线网络连接。在此架构中，利用$D-SDN$实现用户的认证、授权和移动性管理。在初始认证过程中，车载MRN作为普通UE接入网络，随后在切换认证过程中，MRN 作为基站为列车上的用户终端UE提供不间断的网络服务。DgNB作为5G接入网络中的基站被用于实现MRN与$D-SDN$之间的逐跳保护[12]。

4.2.2 设计目标

设计良好的5G高铁网络中MRN的群组切换认证方案应满足以下目标。

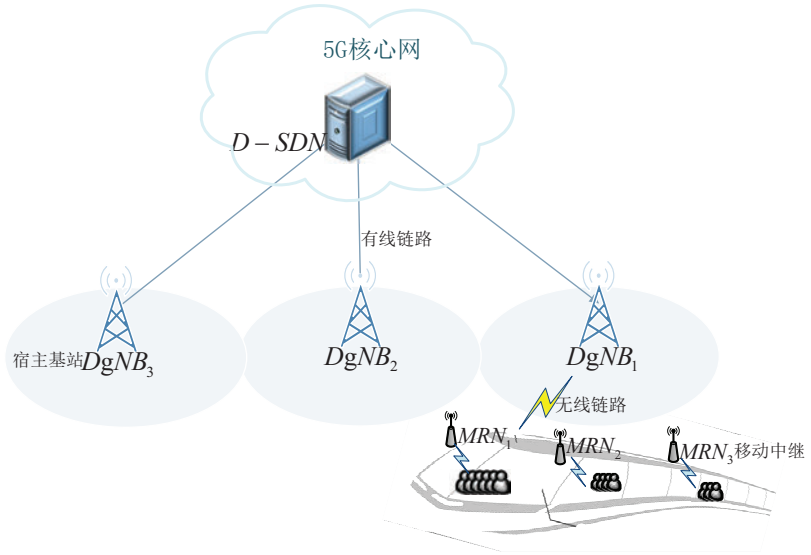


图 4.1　高铁网络架构

安全. 由于MRN是通过不安全的空口信道接入5G网络，MRN的群组切换认证方案应该满足以下几个安全属性。

（1）相互认证

在切换认证过程中，MRN与5G网络都应该验证彼此的合法性，防止攻击者假冒MRN或者网络侧实体去欺骗对方。

（2）密钥协商

在切换认证过程中，MRN与基站应该协商出会话密钥用以保护未来通信数据的机密性。

（3）抵抗重放攻击

在切换认证过程中，应该防止攻击者重放之前已经发送过的数据包给MRN或者基站，从而欺骗MRN或者基站。

性能. MRN的群组切换认证方案应该考虑以下效率需求。

（1）为提高多个MRN并发切换认证的成功率，应尽量减少信令开销，避免信令冲突。

（2）应该在满足高安全性的前提下尽量减少网络通信开销以及MRN和5G网络侧实体的计算开销。

4.2.3　设计思路

本节的设计思路简要描述如下。同一列车上的所有MRN_i可以构成一个MRN群组。不失一般性，假设MRN群成员的个数是n，且MRN_1是群主。在高铁运行过程中，有源供电的MRN_1可以持续监测信号强度、源基站$DgNB_1$的有效覆盖范围、当前地理位置信息以及列车的方向和速度。进而，MRN_1可以根据监测到的数据判断

是否到达切换触发门限（Handover Trigger Threshold，HTT）。例如，假设HTT是列车继续停留在$DgNB_1$的时间少于3秒。一旦HTT满足，MRN_1联合MRN群组成员通过$DgNB_1$给$D-SDN$发送包括轨迹信息在内的用户切换请求消息。

由于高铁的轨迹通常是固定的，$D-SDN$接收到用户切换请求消息后可以存储或者获取所有DgNB的位置信息，决策出MRN群组需要访问的下一个基站$DgNB_2$并协助MRN群组与$DgNB_2$提前执行切换认证过程。由于MRN群组与$DgNB_2$的切换过程是在$DgNB_1$中进行，所以MRN群组可以通过$DgNB_1$获得稳定连续的网络服务。

与此同时，考虑到MRN群组进入$DgNB_2$的覆盖范围后，由于高铁的高速移动性，MRN群组可能会迅速离开$DgNB_2$，进入下一个基站$DgNB_3$的覆盖范围，导致MRN群组在$DgNB_2$无法提前完成与$DgNB_3$的切换认证过程，因此考虑了协同切换认证过程。在协同切换认证过程中，$D-SDN$接收到用户切换请求消息后，根据车辆的路径信息以及$DgNB_2$的位置信息判断协同切换触发门限（Collaborative Handover Trigger Threshold，CHTT）是否也到达。如果CHTT到达，则$D-SDN$决策出MRN群组即将访问的下一个基站$DgNB_2$和下下一个基站$DgNB_3$并协助MRN群组和$DgNB_2$以及$DgNB_3$同时提前执行切换认证过程。在此过程中，MRN群组进入$DgNB_2$的覆盖范围后无需再与$DgNB_3$执行切换认证过程，因此可以避免逗留时间较短无法完成一次切换的问题。

切换认证完成之后，列车上的MRN进入下个基站的覆盖范围可直接与下个基站进行安全通信。与此同时，进入目标基站的覆盖范围后，MRN群主需向$D-SDN$发送切换目标基站的通知。

4.3 第一个方案：FTGPHA1

4.3.1 概述

本小节，介绍了一个低计算开销的群组预切换认证方案。每个MRN_i第一次接入网络时通过执行3GPP认证标准5G-AKA/EAP-AKA'[15, 118]完成初始认证过程。根据5G-AKA认证标准[15]，初始认证过程完成之后，每个MRN以及接入和移动管理实体（Access and Mobility Management Function，AMF）可以获得共享私钥K_{AMF}以及5G网络全球唯一临时终端标识（5G Globally Unique Temporary Identifier，5G-GUTI）。随后，AMF和MRN分别通过K_{AMF}导出下一跳参数（Next Hop，NH），然后AMF将NH和5G-GUTI传输给源基站$DgNB_1$。最后，源基站和MRN通过NH导出会话密钥K_{gNB}用以保护未来通信数据的机密性。

当列车即将离开当前基站$DgNB_1$，MRN群组启动预切换认证过程。在预切换认证过程中，MRN群组将其有效临时终端标识发送给MRN群主MRN_1，MRN_1将

接收到的终端标识信息转发给$D-SDN$。$D-SDN$验证MRN，然后为MRN群组选择合适的目标基站$DgNB_2$，且将新的$NH_i{}^*$发送给$DgNB_2$。随后，MRN群组成员和$DgNB_2$利用新的$NH_i{}^*$计算出会话密钥。方案FTGPHA1的简要概述如图4.2。

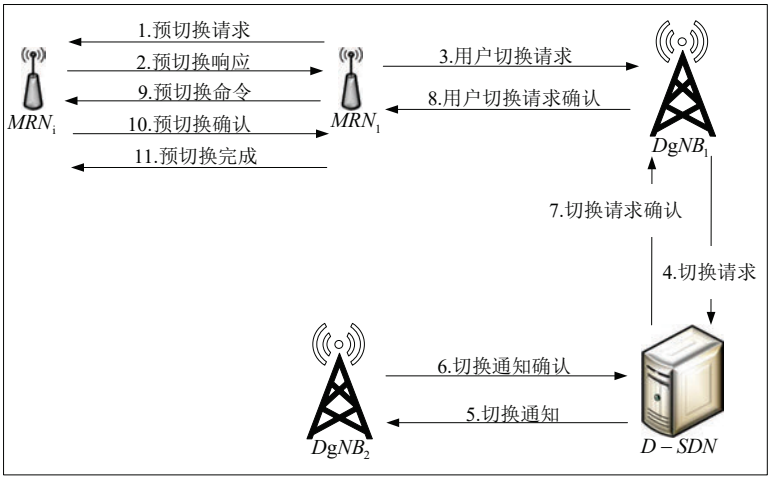


图 4.2　方案FTGPHA1简要概述

4.3.2　具体过程

群组预切换认证过程具体如下：

1. $MRN_1 \rightarrow MRN_i$: 预切换请求(r_M)

   当HTT触发后，MRN_1生成一个随机数r_M并将其广播给群成员。

2. $MRN_i \rightarrow MRN_1$: 预切换响应$(5G-GUTI_i, MAC_i)$

   每个MRN_i接收到广播消息后，计算$MAC_i = h(SUPI_i, NH_i, r_M)$，并生成预切换响应消息给$MRN_1$。预切换响应消息包括临时标识$5G-GUTI_i$和$MAC_i$，其中$SUPI_i$代表与$5G-GUTI_i$相对应的$MRN_i$的用户永久标识，$h()$是一个安全的单向哈希函数。

3. $MRN_1 \rightarrow DgNB_1$: 用户切换请求$((5G-GUTI_i)_{i=1,...,n}, MAC, r_M, other)$

   MRN_1接收到预切换响应消息后，计算$MAC = MAC_1 \oplus MAC_2 \oplus ... \oplus MAC_n$，并且将包含$MAC$、$r_M$、所有$MRN_i$的$5G-GUTI_i$以及其他重要信息（例如列车的位置信息、速度信息、驾驶方向信息等）的用户切换请求消息发送给源基站，其中列车的重要信息会被MRN_1和$DgNB_1$之间的会话密钥K_{gNB_1}加密后传输。

4. $DgNB_1 \rightarrow D-SDN$ 切换请求$((5G-GUTI_i)_{i=1,...,n}, MAC, r_M, other)$

   $DgNB_1$接收到用户切换请求消息后，转发给$D-SDN$。

5. $D-SDN \rightarrow DgNB_2$: 切换通知消息$((5G-GUTI_i{}^*, NH_i{}^*)_{i=1,\ldots,n})$

$D-SDN$接收到切换请求消息后，首先检查r_M是否新鲜，随后根据$5G-GUTI_i$寻找相应的$SUPI_i$以及NH_i，并验证MAC是否正确。如果所有的验证都成功，$D-SDN$基于收集到的列车的路径信息以及基站的位置信息等为MRN群组选择合适的下一个基站$DgNB_2$。随后，$D-SDN$按照等式4-1为每个MRN_i计算一个新的$NH_i{}^*$。另外，$D-SDN$按照等式4-2为每个MRN_i计算一个新的临时标识$5G-GUTI_i{}^*$。随后，$D-SDN$发送一个切换通知信息给$DgNB_2$。切换通知消息内容包括所有的$(5G-GUTI_i{}^*, NH_i{}^*)$，以及其他用于切换的必要信息。

$$NH_i{}^* = KDF(K_{AMF_i}, NH_i, r_M) \tag{4-1}$$

$$5G-GUTI_i{}^* = KDF(SUPI_i, NH_i{}^*, r_M) \tag{4-2}$$

另外，如果检测到CHTT触发，$D-SDN$启动协同切换认证过程。具体地，$D-SDN$为每个MRN_i计算一个新的$NH_i{}^{**}$和$5G-GUTI_i{}^{**}$。随后，$D-SDN$同样发送一个切换通知消息$(5G-GUTI_i{}^{**}, NH_i{}^{**})$给$DgNB_3$。在此情形下，$D-SDN$设置$ContinousChangeBS$值为真。

6. $DgNB_2 \rightarrow D-SDN$: 切换通知确认(m_{gNB_2})

接收到切换通知消息后，$DgNB_2$按照等式4-3为每个MRN_i计算新的会话密钥，并且将$K_{gNB_i}{}^*$与$5G-GUTI_i{}^*$对应。$DgNB_2$可以直接使用$K_{gNB_i}{}^*$作为和MRN_i通信的会话密钥，且采用$5G-GUTI_i{}^*$作为每个MRN_i的临时标识。然后，$DgNB_2$将包含其物理小区标识（Physical Cell ID，PCI）等必要信息的m_{gNB_2}包含在切换通知确认消息中发送给$D-SDN$。最后，$DgNB_2$存储$(5G-GUTI_i{}^*, K_{gNB_i}{}^*)$。

$$K_{gNB_i}{}^* = KDF(NH_i{}^*, PCI, FADL) \tag{4-3}$$

另外，如果$DgNB_3$同样也接收到了切换通知消息，$DgNB_3$执行与$DgNB_2$相同的操作，且发送m_{gNB_3}给$D-SDN$。

7. $D-SDN \rightarrow DgNB_1$: 切换请求确认$(m_{gNB_2}, r_D, MAC^*)/(m_{gNB_2}, m_{gNB_3}, r_D, MAC^*, ContinousChangeBS)$

$D-SDN$接收到切换通知确认消息后，选择一个随机数r_D，按照等式4-4或4-5（如果$ContinousChangeBS$值为真）计算MAC^*。$D-SDN$将m_{gNB_2}，r_D以及MAC^*包含在切换请求确认消中发送给源基站。$h()$是一个安全的单向哈希

函数。如果$ContinousChangeBS$值为真，m_{gNB_3}和标识$ContinousChangeBS$也应该包含在切换请求确认消息中。

$$MAC^* = h(m_{gNB_2}, {NH_1}^*, SUPI_1, r_D) \oplus ...h(m_{gNB_2}, {NH_n}^*, SUPI_n, r_D) \quad (4\text{-}4)$$

$$\begin{aligned} MAC^* = h(m_{gNB_2}, {NH_1}^*, SUPI_1, r_D) \oplus h(m_{gNB_3}, {NH_1}^{**}, SUPI_1, r_D) \oplus \\ ... \oplus h(m_{gNB_2}, {NH_n}^*, SUPI_n, r_D) \oplus h(m_{gNB_3}, {NH_n}^{**}, SUPI_n, r_D) \end{aligned} \quad (4\text{-}5)$$

8. $DgNB_1 \rightarrow MRN_1$: 用户切换请求确认(m_{gNB_2}, r_D, MAC^*)/(m_{gNB_2}, m_{gNB_3},r_D, MAC^*, $ContinousChangeBS$)

   $DgNB_1$将接收到切换请求确认消息转发给MRN_1。

9. $MRN_1 \rightarrow MRN_i$: 预切换命令(m_{gNB_2}, r_D)/(m_{gNB_2}, m_{gNB_3}, r_D, $ContinousChangeBS$)

   MRN_1接收到用户切换请求确认消息后，广播预切换命令消息给MRN组成员，其中消息内容包括(m_{gNB_2}, r_D)或者($m_{gNB_2}, m_{gNB_3}, r_D, ContinousChangeBS$)。

10. $MRN_i \rightarrow MRN_1$: 预切换确认${MAC_i}^*$

    每个MRN_i接收到预切换命令消息后，首先检查r_D是否新鲜。如果新鲜，每个MRN_i验证值$ContinousChangeBS$是否为真。如果不是真，每个MRN_i按照等式4-1计算一个新的${NH_i}^*$，并且计算${MAC_i}^* = h(m_{gNB_2}, {NH_i}^*, SUPI_i, r_D)$。否则，每个$MRN_i$计算${NH_i}^*$、${NH_i}^{**}$以及${MAC_i}^* = h(m_{gNB_2}, {NH_i}^*, SUPI_i, r_D) \oplus h(m_{gNB_3}, {NH_i}^{**}, SUPI_i, r_D)$。最后，每个$MRN_i$将${MAC_i}^*$传输给$MRN_1$。

11. MRN_1接收到预切换确认消息后，验证等式4-6的有效性。如果验证通过，MRN_1发送一个预切换完成消息给每个MRN_i，同时发送切换确认消息给$DgNB_2$。

    $$MAC^* = {MAC_1}^* \oplus {MAC_2}^* ... \oplus {MAC_n}^* \quad (4\text{-}6)$$

    随后，每个MRN_i按照等式4-3计算一个新的用于和$DgNB_2$通信的会话密钥${K_{gNB_i}}^*$，并且按照等式4-2导出临时标识。如果$ContinousChangeBS$ 为真，每个MRN_i计算两组数据：用于MRN_i和$DgNB_2$之间的$({K_{gNB_i}}^*, 5G{-}GUTI_i^*)$，以及用于$MRN_i$ 和$DgNB_3$ 之间的$({K_{gNB_i}}^{**}, 5G{-}GUTI_i^{**})$。下一个基站接收到切换确认消息后，为每个$MRN_i$准备接入控制。

在预切换步骤完成之后，一旦列车进入到下一个基站$DgNB_2$/$DgNB_3$的范围，每个MRN_i与下一个基站可以直接使用会话密钥${K_{gNB_i}}^*$/${K_{gNB_i}}^{**}$保护通信数据的机密性。

4.4 第二个方案：FTGPHA2

4.4.1 概述

在本小节，介绍了一个安全的群组预切换认证协议：FTGPHA2。FTGPHA2的认证开销大于第一个方案FTGPHA1的认证开销，但是FTGPHA2可以实现更健壮的安全属性。在FTGPHA2，每个MRN_i第一次接入网络时，首先执行初始认证过程。在此过程中，每个MRN_i给$D-SDN$提供其有效的身份标识信息，然后$D-SDN$为每个MRN_i生成有效的公私钥。与此同时，在$D-SDN$的协助下，每个MRN_i与当前基站$DgNB_1$协商会话密钥。当MRN群组即将离开当前基站进入下一个基站的覆盖范围后，MRN群组执行群组预切换认证过程。在此过程中，每个MRN_i加密和签名其隐私信息，随后，群主MRN_1聚合所有的签名消息为一个单一的签名，并把它发送给$D-SDN$。$D-SDN$验证签名，如果验证成功，$D-SDN$选择合适的下一个基站$DgNB_2$并协助$DgNB_2$ 和MRN群组完成会话密钥的协商。方案FTGPHA2简要概述如图4.3所示。表4.1列出了本小节用到的符号定义。

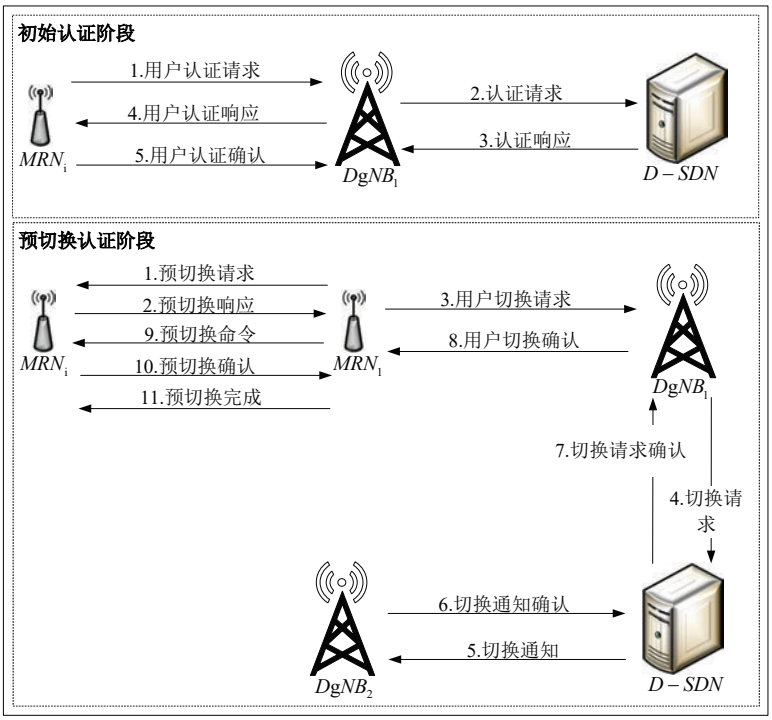


图 4.3 方案FTGPHA2简要概述

4.4.2 具体过程

方案FTGPHA2的具体过程包括下列三个阶段，描述如下。

1. 初始化阶段

在初始化阶段，$D-SDN$选择一个椭圆曲线E上的循环群G。G的生成元是P，

表 4.1　符号定义

符号	定义
E, G	椭圆曲线E上的循环群G
P, q	G的生成元和阶
sk_{SDN}/pk_{SDN}	$D-SDN$的私钥/公钥
sk_i/pk_i	节点i的私钥/公钥
$H_1() - H_6()$	$H_1 : G \rightarrow \{0,1\}^*$,
	$H_2 : G \rightarrow {Z_q}^*$,
	$H_3 : G \times G \times \{0,1\}^* \rightarrow {Z_q}^*$,
	$H_4 : G \times \{0,1\}^* \rightarrow \{0,1\}^*$,
	$H_5 : G \times \{0,1\}^* \times \{0,1\}^* \rightarrow {Z_q}^*$,
	$H_6 : G \times \{0,1\}^* \times G \times \{0,1\}^* \times \{0,1\}^* \rightarrow {Z_q}^*$

阶是q。另外，$D-SDN$选择一个随机数$sk_{SDN} \in {Z_q}^*$作为主私钥，pk_{SDN}作为公钥，其中$pk_{SDN} = sk_{SDN} * P$。随后，$D-SDN$选择6个安全的哈希函数，H_1，H_2，H_3，H_4，H_5和H_6。最后，$D-SDN$ 公开参数$(G, P, q, H_1, H_2, H_3, H_4, H_5, H_6)$。

2. 初始认证阶段

当每个MRN_i第一次接入5G网络时，它需要与$D-SDN$执行初始认证过程，具体如下。

(1) $MRN_i \rightarrow DgNB_1$: 用户认证请求(C_i,K_i)

MRN_i随机选择一个值$k_i \in {Z_q}^*$，按照等式4-7计算U_i, K_i以及密文C_i，其中ID_i表示MRN_i的身份标识信息$SUPI_i/5G-GUTI_i$。随后，MRN_i将用户认证请求消息(C_i, K_i)发送给$DgNB_1$。

$$\begin{aligned} U_i &= k_i * pk_{SDN} \\ K_i &= k_i * P \\ C_i &= H_1(U_i) \oplus ID_i \end{aligned} \tag{4-7}$$

(2) $DgNB_1 \rightarrow D-SDN$: 认证请求(C_i,K_i)

$DgNB_1$转发消息给$D-SDN$。

(3) $D-SDN \rightarrow DgNB_1$: 认证响应$(A_i, Y_i, TK_{1-i}, ID_i')$

$D-SDN$接收到来自$DgNB_1$的消息后，按照等式4-8计算U_i'，并且从C_i 中解密得到MRN_i的身份标识ID_i'。

$$\begin{aligned} U_i' &= K_i * sk_{SDN} \\ ID_i' &= H_1(U_i') \oplus C_i \end{aligned} \tag{4-8}$$

然后，$D-SDN$选择一个随机数$y_i \in Z_q^*$，按照等式4-9计算Y_i，MRN_i的公钥pk_i，z_i以及TK_{1-i}。

$$\begin{aligned} Y_i &= y_i * P \\ pk_i &= Y_i + K_i \\ z_i &= y_i + sk_{SDN} * H_3(pk_i, pk_{SDN}, ID_i') \mod q \\ TK_{1-i} &= y_i * K_i \end{aligned} \tag{4-9}$$

另外，为了保证MRN_i私有值z_i的机密性，$D-SDN$采取如下措施。

$$A_i = H_2(U_i') \oplus z_i \tag{4-10}$$

最后，$D-SDN$发送认证响应消息$(A_i, Y_i, TK_{1-i}, ID_i')$给$DgNB_1$并且存储$(ID_i', pk_i)$。

(4) $DgNB_1 \rightarrow MRN_i$: 用户认证响应(A_i, Y_i)

$DgNB_1$存储TK_{1-i}作为和MRN_i的会话密钥，且将ID_i'作为MRN_i的身份标识。随后，$DgNB_1$将用户认证响应消息(A_i, Y_i)转发给MRN_i。

(5) $MRN_i \rightarrow DgNB_1$:用户认证确认

MRN_i接收到消息后，根据等式4-11计算z_i'和pk_i，并且验证z_i'。

$$\begin{aligned} z_i' &= H_2(U_i) \oplus A_i \\ pk_i &= Y_i + K_i \\ z_i' * P &= Y_i + pk_{SDN} * H_3(pk_i, pk_{SDN}, ID_i) \end{aligned} \tag{4-11}$$

如果验证成功，MRN_i按照等式4-12计算会话密钥TK_{1-i}，存储sk_i作为其私钥，pk_i作为其公钥。最后，MRN_i发送一个用户认证确认消息给$DgNB_1$。

$$\begin{aligned} TK_{1-i} &= k_i * Y_i \\ sk_i &= (z_i' + k_i) \, mod \, q \end{aligned} \tag{4-12}$$

初始认证完成之后，会话密钥TK_{1-i}可以用于确保$DgNB_1$和MRN_i之间通信信道的机密性，而公私钥对(sk_i, pk_i)可以用于完成后续预切换认证过程。

3. 预切换认证阶段

MRN_1监测到HTT触发后，执行如下步骤。

(1) $MRN_1 \rightarrow MRN_i$: 预切换请求

MRN_1广播一个预切换请求消息告知所有群成员开始预切换认证过程。

(2) $MRN_i \rightarrow MRN_1$: 预切换响应(X_i, S_i, C_i)

MRN_i接收到预切换请求消息后，选择一个随机数$x_i \in Z_q^*$，按照等式4-13计算X_i, V_i, 签名S_i以及密文C_i，其中M_i代表切换认证的必要信息，例如，MRN_i的5G-GUTI。

$$\begin{aligned} X_i &= x_i * P \\ V_i &= x_i * pk_{SDN} \\ S_i &= x_i + sk_i + H_3(V_i, X_i, M_i) \ mod \ q \\ C_i &= H_1(V_i) \oplus M_i \end{aligned} \tag{4-13}$$

最后，MRN_i发送一个包括(X_i, S_i, C_i)的预切换响应消息给MRN_1。

(3) $MRN_1 \rightarrow DgNB_1$: 用户切换请求$((X_i, C_i)_{i=1,\ldots,n}, sumS, other)$

MRN_1接收到预切换响应消息后，按照等式4-14计算$sumS$。最后，MRN_1 发送用户切换请求消息给$DgNB_1$，消息内容包括$((X_i, C_i)_{i=1,\ldots,n}, sumS)$以及其他用于切换的重要信息，例如列车的位置、速度、方向等信息，并且用户切换请求消息可采用$DgNB_1$和MRN_1之间的会话密钥TK_{1-1}加密后传输。

$$sumS = \sum_{i=1}^{n} S_i \ mod \ q \tag{4-14}$$

(4) $DgNB_1 \rightarrow D-SDN$: 切换请求$((X_i, C_i)_{i=1,\ldots,n}, sumS, other)$

$DgNB_1$接收到用户切换请求消息后，转发给$D-SDN$。

(5) $D-SDN \rightarrow DgNB_2$: 切换确认$((X_i, M_i')_{i=1,\ldots,n})$

$D-SDN$按照等式4-15解密获得所有MRN的隐私信息M_i'。

$$\begin{aligned} V_i' &= X_i * sk_{SDN} \\ M_i' &= H_1(V_i') \oplus C_i \end{aligned} \tag{4-15}$$

然后，$D-SDN$从M_i'中解析出ID_i'，然后根据ID_i'在其数据库中搜索每个MRN_i的公钥pk_i。随后，$D-SDN$按照等式4-16认证MRN群组。如果认证成功，$D-SDN$基于已有的路径信息为MRN群组选择合适的下一个基站$DgNB_2$，并且通过已经提前建立好的安全信道将切换通知消息$((X_i, M_i')_{i=1,\ldots,n})$发送给$DgNB_2$。

$$\begin{aligned} sumS * P = &\sum_{i=1}^{n} X_i + \sum_{i=1}^{n} pk_i + (\sum_{i=1}^{n} H_3(V_i', X_i, M_i') \ mod \ q) * P \\ &+ (\sum_{i=1}^{n} H_3(pk_i, pk_{SDN}, ID_i') \ mod \ q) * pk_{SDN} \end{aligned} \tag{4-16}$$

另外，如果$D-SDN$监测到CHTT也触发了，则$D-SDN$启动协同切换认证过程。具体地，$D-SDN$同样将切换通知消息$((X_i, M'_i)_{i=1,...,n})$发送给$DgNB_3$。在此情形下，$D-SDN$设置$ContinousChangeBS$为真.

(6) $DgNB_2 \rightarrow D-SDN$: 切换通知确认(R, m_{gNB_2}, HV)

$DgNB_2$接收到切换通知消息后，随机选择一个值$r \in Z_q^*$，按照如下等式计算R，并且为每个MRN_i计算会话密钥TK_{2-i}。

$$\begin{aligned} R &= r * P \\ TK_{2-i} &= r * X_i \end{aligned} \tag{4-17}$$

随后，$DgNB_2$按照如下等式计算哈希值HV。

$$HV = H_4(TK_{2-1}, M'_1) \oplus ... \oplus H_4(TK_{2-n}, M'_n) \tag{4-18}$$

最后，$DgNB_2$将切换通知确认消息(R, m_{gNB_2}, HV)发送给$D-SDN$。

另外，如果$DgNB_3$也接收到了切换通知消息，$DgNB_3$执行与$DgNB_2$相同的操作，并且传输(R^*, m_{gNB_3}, HV^*)给$D-SDN$。

(7) $D-SDN \rightarrow DgNB_1$: 切换请求确认$(R, m_{gNB_2}, HV')/(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'', ContinousChangeBS)$

$D-SDN$接收到切换通知确认消息后，如果$ContinousChangeBS$不为真，直接转发消息(R, m_{gNB_2}, HV')给$DgNB_1$，其中哈希值HV'计算公式如等式4-19。

$$HV' = H_5(R, m_{gNB_2}, HV) \tag{4-19}$$

如果$ContinousChangeBS$为真，$D-SDN$将接收到的两个消息聚合为一个消息$(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'')$，并且传输一个切换请求确认消息$(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'', ContinousChangeBS)$给$DgNB_1$，其中哈希值$HV''$的计算过程如等式4-20。

$$HV'' = H_6(R, m_{gNB_2}, R^*, m_{gNB_3}, HV \oplus HV^*) \tag{4-20}$$

(8) $DgNB_1 \rightarrow MRN_1$: 用户切换请求确认$(R, m_{gNB_2}, HV')/(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'', ContinousChangeBS)$

$DgNB_1$接收到切换请求确认消息后，转发给MRN_1。

(9) $MRN_1 \rightarrow MRN_i$: 预切换命令$(R)/(R, R^*, ContinousChangeBS)$

MRN_1广播预切换命令消息$(R)/(R, R^*, ContinousChangeBS)$ 给所有MRN群成员。

(10) $MRN_i \rightarrow MRN_1$: 预切换确认(RES_i)

MRN_i接收到R后，如果$ContinousChangeBS$不为真，直接计算会话密钥TK_{2-i}并且生成一个预切换确认消息RES_i。

$$\begin{aligned} TK_{2-i} &= R * x_i \\ RES_i &= H_4(TK_{2-i}, M_i) \end{aligned} \tag{4-21}$$

如果$ContinousChangeBS$为真，每个MRN_i需要计算两组会话密钥值：用于和$DgNB_2$之间的$TK_{2-i} = R * x_i$，以及用于和$DgNB_3$之间的$TK_{3-i} = R^* * x_i$。然后，MRN_i按照等式4-22生成一个预切换确认消息RES_i。

$$RES_i = H_4(TK_{2-i}, M_i) \oplus H_4(TK_{3-i}, M_i) \tag{4-22}$$

最后，MRN_i将RES_i发送给MRN_1。

(11) MRN_1接收到所有的RES_i后，如果$ContinousChangeBS$不为真，按照等式4-23验证哈希值HV'。

$$\begin{aligned} RES &= RES_1 \oplus ... \oplus RES_n \\ HV' &= H_5(R, m_{gNB_2}, RES) \end{aligned} \tag{4-23}$$

如果$ContinousChangeBS$为真，MRN_1按照等式4-24验证哈希值HV''。

$$HV'' = H_6(R, m_{gNB_2}, R^*, m_{gNB_3}, RES) \tag{4-24}$$

如果验证成功，MRN_1发送一个预切换完成消息$m_{gNB_2}/(m_{gNB_2}, m_{gNB_3})$给其所有群成员，且发送一个切换确认消息给$D-SDN$，通知$D-SDN$预切换认证过程成功完成。

预切换过程完成之后，当列车进入目标基站$DgNB_2/DgNB_3$的覆盖范围，每个MRN_i和$DgNB_2/DgNB_3$直接采用会话密钥TK_{2-i}/TK_{3-i}保护通信数据的机密性。

4.5 安全评估

本小节，采用形式化验证工具Tamarin和非形式化安全分析证明了提出的两个方案的安全性。

4.5.1 形式化验证工具：Tamarin

在本小节，采用自动化验证工具Tamarin[119]对所提出的方案进行了形式化分析，该工具可以精确地分析各种协议的保密特性和认证特性。Tamarin 模型内置一些常用的密码学操作，例如Diffie-Hellman模指数操作和双线性映射操作等[98]。由于方案FTGPHA1的Tamarin模型类似于FTGPHA2 的模型，这里只详细介绍FTGPHA2的Tamarin模型。在Tamarin模型中，协议采用多个重写规则进行建模，所需的安全属性用$lemma$表示。在具体的Tamarin模型中，All 代表全局量化，Ex 表示存在量化，$\natural$表示时间戳前缀，而F @ $\#i$表示事件F发生在时间点i。在方案FTGPHA2的Tamarin模型中，有两个基本角色*SDN*和*MRN*，多个重写规则$rule$和安全属性$lemma$，具体介绍如下。

四个重写规则：*Setup*、*MRN_1*、*MRN_2*以及*SDN_1*，其中，规则*Setup*用于给SDN和MRN分配公私钥对。

```
rule Setup:
[Fr(~skM),Fr(~xN)] --[Setup()]-> [!Pk($SDN, pmult(~xN,'P')),!Ltk($SDN,~xN),SDN_init
($MRN,pk(~skM)),Out_S($SDN,$MRN,<~skM,pk(~skM)>),Out(pk(~skM))]
```

规则*MRN_1*和*MRN_2*用于定义MRN侧的切换认证过程。

```
rule MRN_1:
let
Xi=pmult(~xi,'P')
Vi=pmult(~xi,XN)
ki=h(<Vi,Xi,~mi>)
ci=~mi XOR h(Vi)
in
[In_S($SDN,$MRN,<~skM,pk(~skM)>)
,!Pk($SDN, XN)
,Fr(~xi)
,Fr(~mi) ]
--[SendRequest($MRN,~mi)]->
[ MRN_1( $SDN, ~mi ,pk(~skM),~xi)
 , Out(<Xi,sign(ki,~skM),ci>)
]

rule MRN_2:
let
key=pmult(~xi,R)
in
[ MRN_1($SDN, ~mi,pk(~skM),~xi)
, In(<R,request>) ]
 --[ RecvConfirm($SDN,R,request), SecretMsg(~mi),SecretPFS(key),
  Eq(request,h(<R,key,~mi>))]->[]
```

规则*SDN_1*用于定义SDN侧的切换认证过程。

```
rule SDN_1:
let
Vi=pmult(~xN,Xi)
mi1=ci XOR h(Vi)
```

```
ki1=h(<Vi,Xi,mi1>)
R=pmult(~r,'P')
key=pmult(~r,Xi)
in
[ !Ltk($SDN,~xN)
 , In( <Xi,si,ci>)
 , SDN_init($MRN,pk(~skM))
 , Fr(~r)]
--[ RecvRequest($MRN,mi1), Eq(verify(si,ki1,pk(~skM)),true), SendConfirm($SDN,R,
h(<R,key,mi1>))]->[Out(<R, h(<R,key,mi1>)>)]
```

在介绍安全属性$lemma$之前，首先介绍Tamarin模型中采用的等式限制。

在方案FTGPHA2中，*SDN*通过验证签名认证*MRN*，且*MRN*通过接收到的哈希值认证*SDN*。分别采用了两个trace去体现这两个认证过程，一个是$verify$ 函数的返回值必须为常量$ture$，例如$Eq(verify(si, ki1, pk(skM)), true)$，另外一个是接收到的哈希值必须等于计算得到的哈希值，例如$Eq(request, h(< R, key, mi >))$。为了达到此目标，定义如下等式限制。

```
restriction Equality:
"All x y #i. Eq(x,y) @i ==> x = y"
```

采用四个$lemma$定义了提出方案的安全属性。第一个$lemma\ SDN_auth_MRN$表示无论$RecvRequest(MRN, m)$行为何时发生，一定有一个*MRN*已经发送过请求消息，或者敌手已经提前针对*MRN*执行过私钥揭露操作。由于*SDN*采用*MRN*的公钥验证签名s_i，例如在$RecvRequest(MRN, m)$操作之前已经执行了$Eq(verify(si, ki1, pk(skM)), true)$ 操作，如果验证失败，此$lemma$必定失败。因此，通过此$lemma$，*SDN*可以检查*MRN*是否合法。

```
lemma SDN_auth_MRN:
" /* Whenever the RecvRequest(MRN,m) action occurs, */
( All MRN  m #i. RecvRequest(MRN, m) @ #i
==>
 /* there is an MRN that has sent the request */
 ( (Ex #a. SendRequest(MRN, m) @ a)
/* or the adversary performed a private key reveal on MRN before the
RecvRequest(MRN,m) action occurs*/
 | (Ex #r. LtkReveal(MRN) @ r & r < i)))"
```

第二个$lemma\ MRN_auth_SDN_AND_Negotiate_sesskey$代表两部分内容，*MRN*验证*SDN*且*MRN*与*SDN*协商出相同的会话密钥。具体地，对于所有*MRN*传输给*SDN*的隐私信息m，以及*MRN*与*SDN*建立的会话密钥，一定有一个服务器已经得到了隐私信息m，计算了相同的会话密钥，且回答了请求消息，或者敌手已经针对*SDN*执行过私钥揭漏操作。在方案FTGPHA2的Tamarin模型中，只有合法的*SDN*可以获得m，所以*MRN*可以通过此lemma认证*SDN*。

```
lemma MRN_auth_SDN_AND_Negotiate_sesskey:
" /* For all 'm' and 'key'*/
( All SDN m key #i. RecvConfirm(SDN, m, key) @ #i
==>
 /* there is a SDN that answered the request */
 ( (Ex #a. SendConfirm(SDN, m, key) @ a)
/* or the adversary performed a private key reveal on SDN before SDN obtained
'm' and 'key'*/
 | (Ex #r. LtkReveal(SDN) @ r & r < i)))"
```

第三个$lemma\ Secrecy_message$表示当$SecretMsg(n)$行为在时间点i发生时，敌手不可能获得n，除非敌手已经针对***SDN***执行过私钥揭漏操作。此$lemma$可以用于证明MRN_i隐私信息M_i的机密性。

```
lemma Secrecy_message:
"All n #i. SecretMsg(n) @i ==>(not(Ex #j. K(n) @j))|(Ex SDN #k. LtkReveal(SDN) @k)"
```

第四个$lemma\ Secrecy_PFS$表示当$SecretPFS(key)$行为在时间点i发生，敌手不可能获得会话密钥key，除非敌手在会话密钥建立之前已经针对***SDN***执行过私钥揭漏操作。此$lemma$可以用于证明完美前向安全。

```
lemma Secrecy_PFS:
"All key #i. SecretPFS(key) @i ==>(not(Ex #j. K(key) @j))|(Ex SDN #k. LtkReveal(SDN)
 @k & k<i)"
```

另外，为了确保由于协议未执行而导致的$lemma$无效问题，在上述$lemma$操作之前添加了下述操作。

```
lemma ExecutableRequest:
exists-trace
"Ex MRN m #i #j.SendRequest(MRN,m)@i &RecvRequest(MRN,m)@j"
lemma ExecutableConfirm:
exists-trace
"Ex SDN m n #i #j.RecvConfirm(SDN,m,n)@i & SendConfirm(SDN,m,n)@j"
```

```
==============================================================================
summary of summaries:

analyzed: FTGPHA1_Scheme.spthy

  ExecutableRequest (exists-trace): verified (7 steps)
  ExecutableConfirm (exists-trace): verified (10 steps)
  SDN_auth_MRN (all-traces): verified (7 steps)
  MRN_auth_SDN_AND_Negotiate_sesskey (all-traces): verified (7 steps)
  Secrecy_message (all-traces): verified (3 steps)

==============================================================================
```

图 4.4 方案FTGPHA1的Tamarin运行结果

方案FTGPHA1在Tamarin 2.7.1上的运行结果如图4.4所示，其中$Secrecy_message$用于证明MRN_i身份信息$SUPI_i$的机密性。从图4.4可知，方案FTGPHA1可以成功实现相互认证、密钥协商以及部分匿名性。

方案FTGPHA2在Tamarin 2.7.1上的运行结果如图4.5所示。从图4.5可知，方案FTGPHA2可以实现相互认证、密钥协商、隐私保护和完美前向安全。

图 4.5　方案FTGPHA2的Tamarin运行结果

4.5.2　非形式化安全分析

本小节，分析了方案FTGPHA1和方案FTGPHA2的安全性。

（1）相互认证

对于方案FTGPHA1，只有合法的MRN_i和$D-SDN$才拥有$SUPI_i$ 和NH_i。在预切换过程中，每个MRN_i采用$SUPI_i$和NH_i生成有效的MAC_i，并且MRN 群主聚合所有的MAC_i为一个单一的MAC。$D-SDN$通过检查聚合MAC的有效性认证MRN群组。一旦存在一个无效的MAC_i，认证就会失败。同样地，MRN群组通过检查MAC^*的有效性认证$D-SDN$。

对于方案FTGPHA2，一方面，每个MRN_i利用自己的私钥sk_i生成签名S_i，随后MRN群主MRN_1聚合所有的签名为一个单一的签名$sumS$。$D-SDN$验证聚合签名的有效性。一旦存在无效的签名，验证就会失败。只有合法的MRN_i可以生成有效的签名，进而导出有效的聚合签名。因此，$D-SDN$可以通过检查聚合签名的有效性认证MRN群组。另外一方面，由于每个MRN_i用$D-SDN$的公钥pk_{SDN}加密其隐私信息M_i，只有指定的$D-SDN$才可以获得M_i进而生成有效的哈希值HV'。因此，MRN群组可以通过检验哈希值的正确性认证$D-SDN$。

因此，提出的两个方案均可以实现相互认证。

（2）密钥协商

对于方案FTGPHA1，每个MRN_i和$D-SDN$首先使用密钥K_{AMF_i} 和NH参数NH_i派生出下一个NH参数$NH_i{}^*$。然后，$D-SDN$通过预先建立的安全通道将所有的$NH_i{}^*$安全地传输给$DgNB_2$。随后，每个MRN_i和$DgNB_2$从$NH_i{}^*$ 派生出会话密钥$K_{gNB_i}{}^*$。如果没有$NH_i{}^*$，任何攻击者都无法计算出会话密钥$K_{gNB_i}{}^*$。

对于方案FTGPHA2，每个MRN_i将X_i传输给$DgNB_2$，而$DgNB_2$ 将R传输给MRN群组。随后，$DgNB_2$和MRN群组通过等式$TK_{2-i} = R * x_i = r * X_i$计算会话密钥$TK_{2-i}$，其中参数$r$和$x_i$分别是$DgNB_2$和$MRN_i$的秘密值。通过公开参数$X_i$和$R$ 计算出会话密钥TK_{2-i}相当于求解ECDHP或ECDLP。

因此，提出的两个方案均可以安全地协商出会话密钥。

（3）匿名性和不可链接性

对于方案FTGPHA1，采用临时值$5G-GUTI_i$实现了预切换过程中用户隐私信息的匿名性。但是，由于$5G-GUTI_i$在某段时间内可能不会更新，敌手仍然有可能区分或者追踪MRN_i，因此，该方案可以实现匿名性，但是不能实现不可链接性。

对于方案FTGPHA2，由于MRN_i的隐私信息M_i通过$D-SDN$的公钥pk_{SDN}加密后公开传输，攻击者不可能得到MRN_i的隐私信息。另外，由于在每个会话中，都采用了新鲜的随机数生成消息(X_i, S_i, C_i)，攻击者很难确定两条消息是否来自同一个MRN。因此，该方案可以实现匿名性和不可链接性。

（4）完美前向、后向安全

对于方案FTGPHA1，MRN与基站之间的会话密钥$K_{gNB_i}{}^*$的协商依赖于私有值K_{AMF_i}。一旦K_{AMF_i}泄露，攻击者就能计算出$K_{gNB_i}{}^*$。因此，该方案不能实现完美前向、后向安全。

对于方案FTGPHA2，会话密钥TK_{2-i}是通过等式$TK_{2-i} = R * x_i$或$TK_{2-i} = r * X_i$计算得到的。即使MRN_i的私钥sk_i泄露，由于只有MRN_i 和$D-SDN$拥有值V_i，攻击者不可能从等式$S_i = x_i + sk_i + H_3(V_i, X_i, M_i)\ mod\ q$中获得参数$x_i$，进而计算出会话密钥$TK_{2-i}$。类似地，即使$D-SDN$的私钥$sk_{SDN}$泄露，攻击者也不可能获得参数$r$，进而导出会话密钥$TK_{2-i}$。因此，该方案可以成功实现完美前向、后向安全。

（5）前后密钥分离[120]

对于方案FTGPHA1，在每次预切换认证过程中，$D-SDN$和MRN_i分别利用其私有值K_{AMF_i}生成新的$NH_i{}^*$，随后$D-SDN$将$NH_i{}^*$安全地传输给$DgNB_2$。MRN_i和$DgNB_2$使用新的$NH_i{}^*$计算出会话密钥$K_{gNB_i}{}^*$。即使当前的NH值或会话密钥泄露，攻击者没有K_{AMF_i}也不可能算出之前或者之后的会话密钥。因此，该方案可以保证前后密钥分离。

对于方案FTGPHA2，由于在计算会话密钥TK_{2-i}的过程中采用了新鲜的随机数x_i和r，每个会话中的会话密钥彼此独立。攻击者即使获取了当前的会话密钥，也不可能获得之前或者之后的会话密钥。因此，该方案可以成功实现前后密钥分离。

（6）抵抗重放攻击

对于方案FTGPHA1，由于在每个预切换认证过程中均采用了新的随机数r_M和r_D，因此，该方案可以抵抗重放攻击。

对于方案FTGPHA2，由于在每条会话消息中都采用了随机数x_i 和r，因此，该方案可以抵抗重放攻击。

（7）抵抗假冒攻击

对于方案FTGPHA1，一方面，由于每个MRN_i和$D-SDN$都会利用私有值$SUPI_i$和NH_i生成有效的哈希值，任何敌手都不可能产生有效的哈希值，进而伪造为

合法的$DgNB_2$或MRN_i。另外一方面，任何敌手没有$NH_i{}^*$都不可能获得会话密钥$K^*_{gNB_2}$，也不可能伪造为合法的$DgNB_2$或者MRN_i。因此，该方案可以抵抗假冒攻击。

对于方案FTGPHA2，一方面，只有合法的MRN_i拥有私钥sk_i，且任何敌手没有有效的私钥都不可能伪造出合法的签名。另外，由于$D-SDN$的公钥pk_{SDN}已经被提前预置到MRN设备中，且每个MRN_i均采用pk_{SDN}加密其隐私消息M_i，任何敌手没有对应的私钥sk_{SDN}不可能获得M_i，进而导出有效的哈希值HV'。另外一方面，如上所述，任何敌手都不可能获得会话密钥TK_{2-i}，也不可能伪造为合法的$DgNB_2$或者MRN_i。因此，该方案可以抵抗假冒攻击。

（8）抵抗中间人攻击

对于方案FTGPHA1，没有相应的$SUPI_i$和NH_i，任何敌手都不可能伪造为合法的MRN_i或$D-SDN$去欺骗对方。因此，该方案可以抵抗中间人攻击。

对于方案FTGPHA2，一方面，没有与公钥pk_{SDN}相对应的私钥sk_{SDN}，敌手不可能伪造为合法的$D-SDN$与MRN组成员通信。另外一方面，敌手没有私钥sk_i无法伪造为合法的MRN群成员欺骗$D-SDN$。因此，该方案可以抵抗中间人攻击。

如上所述，方案FTGPHA1无法提供匿名性、不可链路性以及完美前向、后向安全。但是方案FTGPHA2可以成功完成上述所有安全属性。

4.6　性能分析

在本小节，通过将FTGPHA1和FTGPHA2与这些密切相关的方案：5G方案[14, 15]、Haddad的方案[31]、Lai的方案[65]以及Cao两个方案[30, 114]，进行对比来分析它们的性能。

4.6.1　概述

首先，分别从信令开销、通信开销和计算开销三个方面分析了对比方案的性能。由于我们的方案中引入了协同预切换过程，这里考虑下列两种对比场景：普通预切换场景**Scen1** 和协同预切换场景**Scen2**。场景**Scen1**是指MRN组成员进入下一个基站$DgNB_2$的覆盖范围后不会很快离开，因此无需执行协同预切换过程。**Scen2**场景表示MRN群组成员进入$DgNB_2$的覆盖范围后会迅速离开，进入下下个基站$DgNB_3$的覆盖范围，因此我们的两个方案需执行协同切换过程。在场景**Scen2**中，MRN群组成员实际上连续完成了两个群组预切换认证过程，所以此处用总的开销除以2表示一次预切换认证过程中的平均开销。由于其他对比方案均未考虑协同切换过程，所以他们在场景**Scen2**和场景**Scen1**中具有相同的切换开销。随后，在场景**Scen1**中，对比和分析了相关方案在未知攻击下的性能。

为了公平起见，定义对比方案中的安全级别均等价于AES 128比特。具体地，

假设NH参数以及用于对称加密、解密的密钥为128比特，基于椭圆曲线密码学算法的密钥长度为256比特，基于有限域密码学的公钥长度为3072比特，私钥为256比特[47, 48]。另外，哈希的输出值为128比特，随机数为128比特，时间戳为32比特。由于所有的对比方案都与切换相关，都必须传输切换相关的必要信息，例如5G-GUTI，PCI等，假设此类信息的长度为128 比特。不失一般性，假设MRN群成员的个数是n。

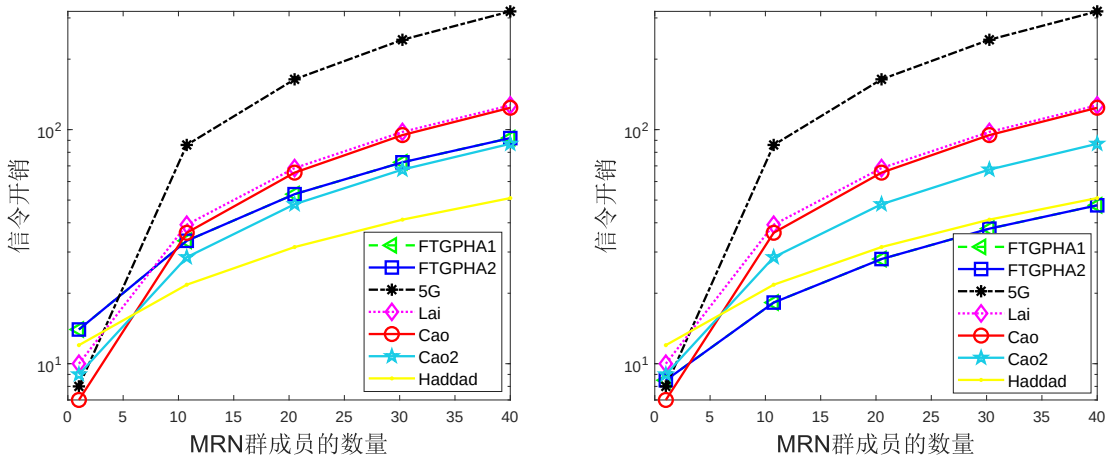
4.6.2 信令开销

在信令开销方面，根据n个MRN的信令消息总数来评估和对比我们方案和其他相关方案。对于方案FTGPHA1和FTGPHA2，在群组预切换认证过程中，群成员和群主MRN_1 之间有$(2n+3)$条消息，群主MRN_1和源基站$DgNB_1$之间有3条消息，源基站$DgNB_1$和$D-SDN$之间有3条消息，$D-SDN$和目的基站$DgNB_2$/$DgNB_3$之间有3条消息。对于5G方案[14, 15]，在一次完整的MME内部切换过程中，UE与源基站之间有2条消息，源基站与MME之间有3条消息，目标基站与MME之间有3条消息，UE 与目标基站之间有1 条消息。对于Lai的方案[65]，在一次群组漫游认证过程中，群成员和群主之间有$(n+1)$条消息，群主和目标基站之间有3条消息，目标基站与MME之间有$(n+3)$条消息，群成员和目标基站之间有n条消息。对于Cao的方案[114]，在一次完整的群组切换认证过程中，群成员和源基站之间有$2n$条消息，源基站和MME之间有2条消息，MME和目的基站之间有2 条消息，群成员和目的基站之间有n条消息。对于Cao的第二个方案[30]，在一次群组切换认证过程中，组成员和群主之间有$(2n+2)$条消息，群主和目标基站之间有3条消息，目标基站和MME之间有2 条消息。对于Haddad的方案[31]，在一次群组切换认证过程中，群组成员和群主之间有$(n+2)$条消息，群主和源基站之间有2条消息，源基站和目标基站之间有3条消息，群主与目标基站之间有2条消息，目标基站与MME之间有2条消息。相关方案的信令开销如表4.2所示。

图4.6列出了我们方案与其他方案在随着MRN群成员数量的增加而产生的信令开销的对比结果。从图4.6(a)可知，我们方案产生的信令开销略大于Haddad的方案[31]中的信令开销，与Cao的第二个方案[30]中的信令开销类似，并且小于其他方案的信令开销。Haddad的方案[31]由于只需每个群成员发起一次请求消息，所以信令开销较少，但是由于采用了较多的双线性映射操作，会产生大量的计算开销。此外，根据图4.6(b)可知，在我们的方案中，通过执行协同切换认证过程可以进一步减少信令开销。原因主要是执行协同切换过程中只需在D-SDN 与$DgNB_3$之间额外交互3条信令消息，所以平均信令开销会明显减少。

表 4.2　n个MRN的信令开销

方案 / 场景	FTGPHA1	FTGPHA2	5G[14, 15]	Lai[65]	Cao[114]	Cao2[30]	Haddad[31]
Scen1	$2n$+12	$2n$+12	$8n$	$3n$+7	$3n$+4	$2n$+7	n+11
Scen2	($2n$+15)/2	($2n$+15)/2	$8n$	$3n$+7	$3n$+4	$2n$+7	n+11



(a) **Scen1**　　(b) **Scen2**

图 4.6　信令开销对比

4.6.3　计算开销

表 4.3　部分密码学操作的计算时间

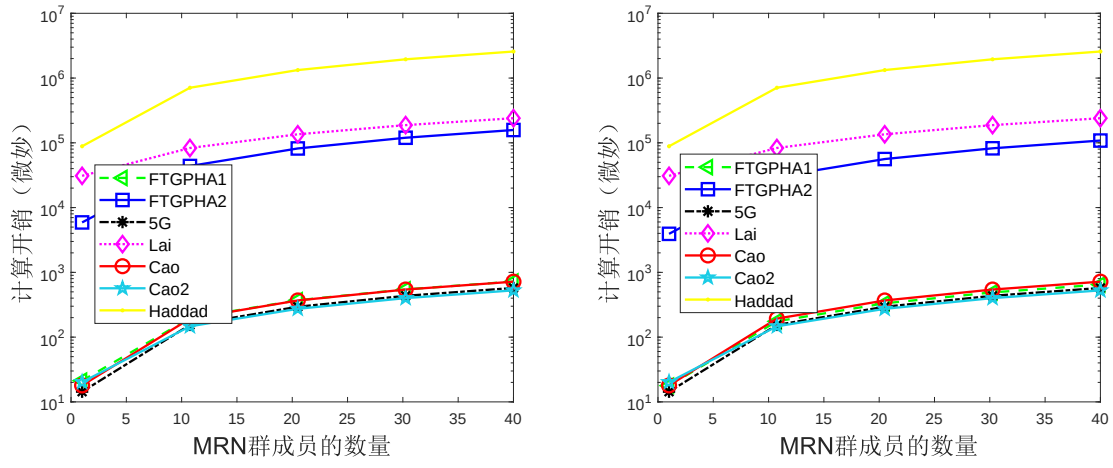
操作(微秒) / 设备	T_M	T_E	T_P	T_A	T_H	T_S
MRN	0.96×10^3	1.89×10^3	1.65×10^4	2.53	2.38	2.26
基站/$D-SDN$	0.50×10^3	1.00×10^3	8.36×10^3	1.39	1.21	1.05

在计算开销方面，只考虑点加操作T_A、点乘操作T_M、模指数操作T_E、双线性映射操作T_P、对称加密/解密操作T_S以及单向哈希操作T_H，而忽略其他耗时较小的操作。我们搭建了一个linux仿真平台采用C/C++ OPENSSL库[110]测试了这些相关密码学操作的计算时间。为了差异化模拟MRN和基站等设备，采用Intel(R) Core(TM) m3-6Y30 CPU 0.9GHz 处理器作为MRN，Intel(R) Core(TM) i7-7500U CPU 2.70GHz处理器作为基站或$D-SDN$。实验结果如表4.3 所示。

表4.4列出了相关方案中分别在两种场景下的n个MRN的总计算开销对比结果。两种场景下随着MRN群成员数量的增加而增加的总计算开销对比结果如图4.7所示。从图4.7(a)可知，在场景**Scen1**中，方案FTGPHA1的计算开销与Cao的两个方案[30, 114]和5G 方案[14, 15]中的计算开销类似，而远小于其他方案。方案FTGPHA2的计算开销大

表 4.4 n个MRN的计算开销

Scen1(微秒)	MRN群组	DgNB和$D-SDN$	总计
FTGPHA1	$5nT_H$+T_S = 11.90n+2.26	$5nT_H$+T_S = 6.05n+1.05	17.95n+3.31
FTGPHA2	$3nT_M$+(3n+1)T_H+T_S= 2.89×$10^3$$n$+4.64	(2n+4)T_M+(4n+1)T_H+(2n+1) T_A+T_S=(1.01n+2.00)×10^3	(3.90n+2.00)×10^3
5G[14, 15]	$4nT_H$=9.52n	$4nT_H$=4.84n	14.36n
Lai[65]	$4nT_M$+2nT_H+(3n-1) T_A= 3.85×$10^3$$n$-2.53	(3n+1)T_M+3nT_H+(3n-2)T_A +3T_P=(1.51n+25.58)×10^3	(5.36n+25.58)×10^3
Cao[114]	5nT_H =11.90n	5nT_H=6.05n	17.95n
Cao2[30]	(4n+2)T_H=9.52n+4.76	(2n+2)T_H+nT_S=3.47n+2.42	12.99n+7.18
Haddad[31]	(3n+1)T_P+2nT_E+4nT_H+ nT_M=(5.42n+1.65)×10^4	(n+1)T_P+nT_E+nT_H =(9.36n+8.36)×10^3	(6.36n+2.49)×10^4
Scen2(微秒)	MRN群组	DgNB和$D-SDN$	总计
FTGPHA1	(9nT_H+T_S)/2=10.71n+1.13	(9nT_H + T_S)/2=5.45n+0.53	16.16n+1.66
FTGPHA2	(4nT_M+(4n+1)T_H+T_S)/2 =1.92×$10^3$$n$+2.32	((3n+5)T_M+(5n+1)T_H+(2n+1) T_A+T_S)/2=(0.75n+1.25)×10^3	(2.67n+1.25)×10^3
5G[14, 15]	$4nT_H$=9.52n	$4nT_H$=4.84n	14.36n
Lai[65]	$4nT_M$+2nT_H+(3n-1)T_A= 3.85×$10^3$$n$-2.53	(3n+1)T_M+3nT_H+(3n-2)T_A+ 3T_P=(1.51n+25.58)×10^3	(5.36n+25.58)×10^3
Cao[114]	5nT_H=11.90n	5nT_H=6.05n	17.95n
Cao2[30]	(4n+2)T_H=9.52n+4.76	(2n+2)T_H+nT_S=3.47n+2.42	12.99n+7.18
Haddad[31]	(3n+1)T_P+2nT_E+4nT_H+ nT_M=(5.42n+1.65)×10^4	(n+1)T_P+nT_E+nT_H= (9.36n+8.36)×10^3	(6.36n+2.49)×10^4



(a) **Scen1** (b) **Scen2**

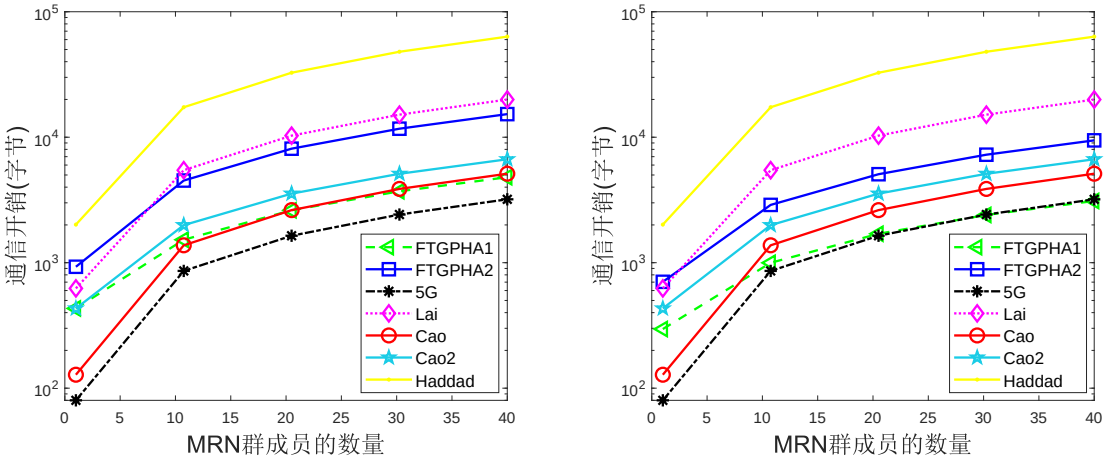
图 4.7 计算开销对比

于方案FTGPHA1，Cao的两个方案[30, 114]以及5G 方案[14, 15]，而小于其他方案。原因包括以下两个方面：一方面，方案FTGPHA1、Cao的两个方案[30, 114] 以及5G方案[14, 15]都只执行了一些简单的哈希操作和对称加解密操作，所以计算开销类似且都较小，但是方案FTGPHA1比Cao的两个方案[30, 114] 以及5G方案[14, 15]都提供更加健壮的安全性；另一方面，方案FTGPHA2和Lai的方案[65]采用了多个点乘操作，所以耗时较多，而Haddad的方案[31]采用了多个双线性映射操作，所以耗时最多。此外，从图4.7(b)可知，在场景**Scen2**中，由于协同切换的引入，方案FTGPHA1 和FTGPHA2 在一次预切换过程中的平均计算开销明显减少。原因主要是协同切换的引入后，MRN群组侧以及DgNB和D-SDN侧无需再次执行认证操作，只需多一次密钥协商操作，所以平均计算开销会明显减少。

4.6.4　通信开销

表 4.5　n个MRN的通信开销

(字节)	FTGPHA1	FTGPHA2	5G[14, 15]	Lai[65]	Cao[114]	Cao2[30]	Haddad[31]
Scen1	112n+320	368n+560	80n	496n+128	128n	160n+272	1572n+440
Scen2	72n+224	224n+480	80n	496n+128	128n	160n+272	1572n+440



(a) **Scen1**　　(b) **Scen2**

图 4.8　通信开销对比

在通信开销方面，如表4.5所示，主要分析对比方案中传输n个MRN的消息总大小。对于方案FTGPHA1，5G方案[14, 15]以及Cao的两个方案[30, 114]，由于传输的消息主要包括随机数、对称加密后的密文以及哈希的输出结果，这些方案的通信开销相对较小。对于方案FTGPHA2，Lai的方案[65]以及Haddad的方案[31]，由于他们的切换认证算法均基于椭圆曲线密码学或者有限域密码学，通信开销都相对较大。

图4.10显示了这些相关方案中随着MRN群成员数量增加的通信开销的对比结果。从图4.8(a) 可知，FTGPHA1 的通信开销稍大于5G 方案[14, 15]，而远小于其他相关方案。方案FTGPHA2比方案FTGPHA1，Cao的两个方案[30, 114] 以及5G 方案[14, 15]耗费更多的通信开销，而比Haddad的方案[31]和Lai的方案[65]耗费更少的通信开销。但是，方案FTGPHA1比5G方案[14, 15]以及Cao的两个方案[30, 114]实现了更多的安全属性且方案FTGPHA2比方案FTGPHA1，Cao的两个方案[30, 114]、5G方案[14, 15]以及Lai的方案[65]都实现了更多的安全属性。

另外，根据图4.8(b)可知，由于协同切换的引入，方案FTGPHA1和FTGPHA2在一次预切换过程中的平均通信开销明显减少。原因主要是协同切换的引入后，MRN群组侧以及DgNB和D-SDN侧无需再次传输认证参数，只需传输密钥协商参数，所以平均通信开销明显减少。

4.6.5 未知攻击下的性能分析

尽管前面已经证明了我们的方案可以抵抗几种已知攻击，但是仍然存在一些不知道何时、何地发生的未知攻击，且无法判定我们的方案是否可以抵抗该类未知攻击。因此，在本小节，评估了未知攻击下的性能。这里只详细介绍未知攻击下通信开销的计算过程，未知攻击下信令开销和计算开销的计算过程与未知攻击下通信开销的计算过程类似。

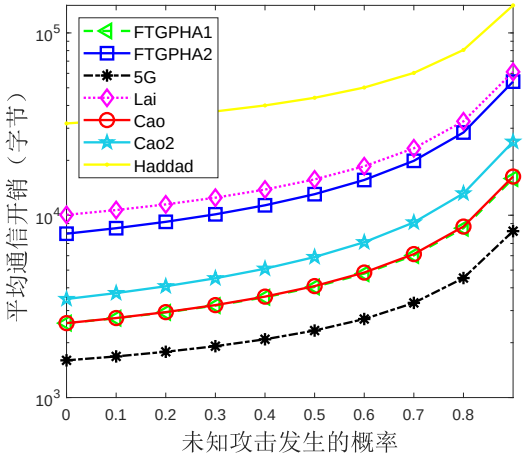


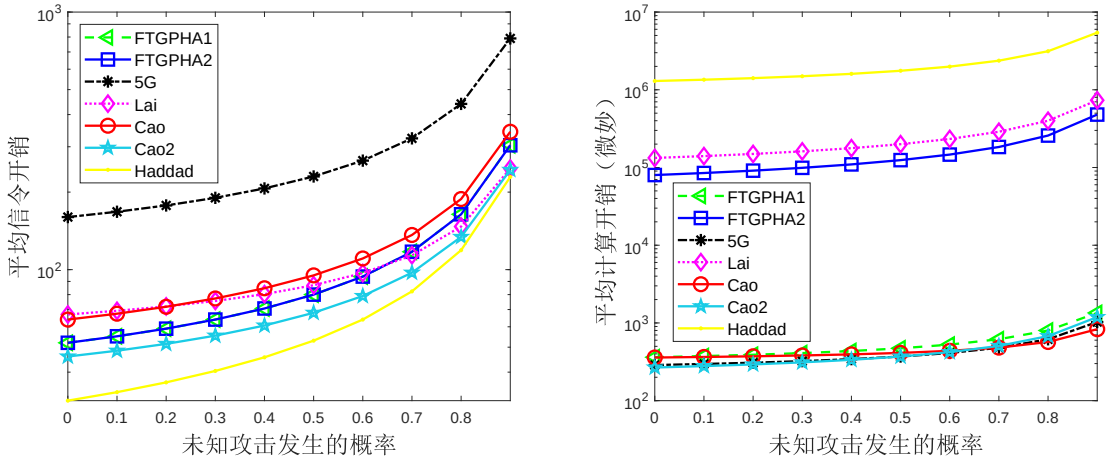
图 4.9 未知攻击下的通信开销对比

$$CO_{avg} = \frac{CO_{fail} * p_{fail} + CO_{succ} * p_{succ}}{p_{succ}} \tag{4-25}$$

具体计算公式如等式4-25所示，其中CO_{avg}代表多个成功或者失败的预切换认证过程的平均通信开销，CO_{fail}代表在未知攻击下一次失败的预切换认证过程的通信开销，p_{fail}代表在协议执行的过程中未知攻击发生的概率，CO_{succ}代表一次成功预

切换认证过程的通信开销且$p_{succ}=1-p_{fail}$。另外，假设在一次预切换认证过程中的总消息个数为N_{total}，且未知攻击发生在第i步的概率为$q=1/N_{total}$。因此，CO_{fail}的计算公式如等式4-26所示，其中CO_i代表未知攻击发生在第i步前的总通信开销。

$$CO_{fail}=\sum_{i=1}^{N_{total}} CO_i * q \tag{4-26}$$



(a) 未知攻击下的信令开销对比　　(b) 未知攻击下的计算开销对比

图 4.10　未知攻击下的信令开销和计算开销对比

图4.9、图4.10(a)以及图4.10(b)分别显示了随着未知攻击发生概率增加的情况下的平均通信开销、信令开销和计算开销的对比结果。为了简化分析，设置$n=20$[30]。从图4.9可知，在未知攻击下，方案FTGPHA1的平均通信开销稍大于5G方案[14, 15]中的平均通信开销，与Cao的第一个方案[114]中的平均通信开销类似，而远小于其他方案中的平均通信开销。另外，在未知攻击下，方案FTGPHA2的平均通信开销大于方案FTGPHA1，Cao的两个方案[30, 114]和5G方案[14, 15]中的平均通信开销，而远小于其他方案的平均通信开销。从图4.10(a)可知，在未知攻击下，方案FTGPHA1和FTGPHA2的平均信令开销大于Cao的第二个方案[30]和Haddad的方案[31]中的平均信令开销，而小于其他方案的平均信令开销。从图4.10(b)可知，在未知攻击下，方案FTGPHA1的平均计算开销与Cao的两个方案[30, 114]以及5G方案[14, 15]中的平均计算开销类似，而远小于其他方案的平均计算开销。方案FTGPHA2的平均计算开销大于方案FTGPHA1，Cao的两个方案[30, 114]以及5G方案[14, 15]中的平均计算开销，而远小于其他方案的平均计算开销。

安全和性能讨论： 表4.6列出了我们提出的两个方案和其他相关方案在性能和安全性方面的对比结果。根据表4.6可知，方案FTGPHA1比5G方案[14, 15]、Cao的两个方案[30, 114]，以及Lai的方案[65]具备更好的安全性能。同时，方案FTGPHA1比5G方案耗费更少的计算开销和通信开销。方案FTGPHA2比除了Haddad的方案[31] 之外的其

表 4.6 安全和性能对比

方案 / 安全属性	FTGPHA1	FTGPHA2	5G[14, 15]	Lai[65]	Cao[114]	Cao2[30]	Haddad[31]
相互认证	√	√	×	×	×	√	√
密钥协商	√	√	√	√	√	√	√
匿名性	√	√	×	×	×	×	√
不可链路性	×	√	×	×	×	×	√
完美前向、后向安全	×	√	×	√	×	×	√
前后密钥分离	√	√	×	√	×	×	√
抵抗协议攻击	√	√	×	×	×	√	√
信令开销	中	中	高	中	中	中	低
计算开销	低	中	低	中	低	低	高
通信开销	低	中	低	中	低	低	高
未知攻击下信令开销	低	低	高	低	低	低	低
未知攻击下计算开销	低	中	低	中	低	低	高
未知攻击下通信开销	低	中	低	中	低	低	高

他方案提供更强的安全属性，但是比Haddad的方案[31]耗费更少的计算开销和通信开销。

本章节提出的方案FTGPHA1和方案FTGPHA2的对比结果如下。在信令开销方面，FTGPHA1 和FTGPHA2所耗费的信令开销相同。在通信开销方面，由于方案FTGPHA1在预切换认证过程中主要传输一些简单的随机数、对称加密密文以及哈希值的输出，但是方案FTGPHA2主要传输椭圆曲线密码学上的参数，方案FTGPHA1的通信开销远小于方案FTGPHA2的通信开销。在计算开销方面，由于FTGPHA1 只执行了一些耗时很小的哈希和对称加密、解密操作，而方案FTGPHA2执行了耗时较多的椭圆曲线密码学上的点乘操作等，因此，方案FTGPHA2的计算开销远大于方案FTGPHA1。在安全方面，方案FTGPHA1 可以提供的安全属性包括相互认证、密钥协商、前后密钥分离以及抵抗多种协议攻击，但方案FTGPHA1不能实现匿名性、不可链路性以及完美前向、后向安全，而方案FTGPHA2可以实现上述所有安全属性。综上所述，方案FTGPHA1适合资源受限，用户性能较差以及安全性需求较低的场景，而方案FTGPHA2适合用户性能较强，安全需求较高以及通信资源较为充裕的场景。

4.7　结论

本章节针对5G高铁网络提出了两个群组预切换认证方案：FTGPHA1 和FTGPHA2。方案FTGPHA1中借鉴了5G网络中MME内部切换认证过程实现了预切换认证过程，而方案FTGPHA2利用了聚合签密技术实现了预切换认证过程。在提出的两个方案中，在$D-SDN$的协助下，MRN群组和目标基站可以在MRN群组到达目标基站覆盖范围之前提前执行预切换认证过程，因此可为用户终端提供较为平滑的通信体验。安全和性能评估结果显示方案FTGPHA1在通信和计算开销方面更加高效，而方案FTGPHA2提供更健壮的安全属性，且耗费合理的切换开销。

第五章　卫星接入网络中终端接入认证方案

为解决5G网络中引入卫星接入技术导致的新的安全问题、终端认证时延过长以及海量IoTD并发接入卫星网络导致信令冲突等问题，本章节提出了一个基于格的接入认证方案。该方案针对海量IoTD 和单个ME或单个IoTD提出了两种不同的协议：海量IoTD的接入认证协议以及单个ME/IoTD的接入认证协议。在海量IoTD的接入认证协议中，海量IoTD构成一个临时群组执行群组认证过程以此克服信令冲突问题。通过利用提出的半聚合签名机制以及会话密钥协商机制，提出的群组方案可以有效降低传输负荷。另外，提出的方案可以快速完成地面站与每个IoTD之间的密钥协商。

5.1　简介

近些年来，学术界的研究者已经提出了多个卫星网络认证方案[32–41]，但是现有方案存在各种各样的安全和性能缺陷。例如，Meng等人[39]，Xue等人[40] 以及Yang等人[41]分别提出了一个安全的卫星网络认证方案，但是文献[39, 40]中的方案并未实现不可链路性以及完美前向、后向安全，且文献[41]中的方案由于使用了多个点乘和双线性映射操作耗费了大量的计算开销。此外，目前所有现有方案都是针对单个设备而设计的，无法避免海量设备并发接入卫星网络时导致的信令冲突问题。因此，研究适用于5G卫星网络的海量终端和单个实体的接入认证方案是十分必要的。

本章节，提出了一个统一、安全的接入认证方案。考虑到近年来量子计算机的快速发展提出了新的挑战。NIST指出，如果大规模的量子计算机被成功部署，基于数论问题的传统方案，例如RSA很容易被破解[43]。此外，NIST还强调，现在必须开始准备能够抵抗量子计算的方案，因为从目前广泛使用的密码系统安全、顺利地迁移到抗量子计算的密码系统需要付出巨大的努力。由于基于格理论的密码学被广泛认为是能够抵抗量子攻击的主要技术之一[43]，因此，研究基于格的接入认证方案。该方案包括两种协议：海量IoTD的接入认证协议以及单个ME/IoTD的接入认证协议。在此方案中，IoTD、ME、卫星以及GS首先注册到NCC 获得其公私钥对，然后GS与其所管辖的卫星采用公私钥对建立一条安全的数据通道。当海量IoTD 并发接入网络时执行海量IoTD的接入认证协议，而当单个IoTD/ME接入网络时执行单个ME/IoTD的接入认证协议。

5.2 系统模型、设计目标和设计思路

本小节，详细描述了系统模型、设计目标以及设计思路。

5.2.1 系统模型

如图5.1所示，偏远地区的IoTD或ME可以通过卫星网络接入陆地通信网络。卫星网络包括NCC、卫星、GS和陆地-卫星终端（Terrestrial-Satellite Terminals，TST）。

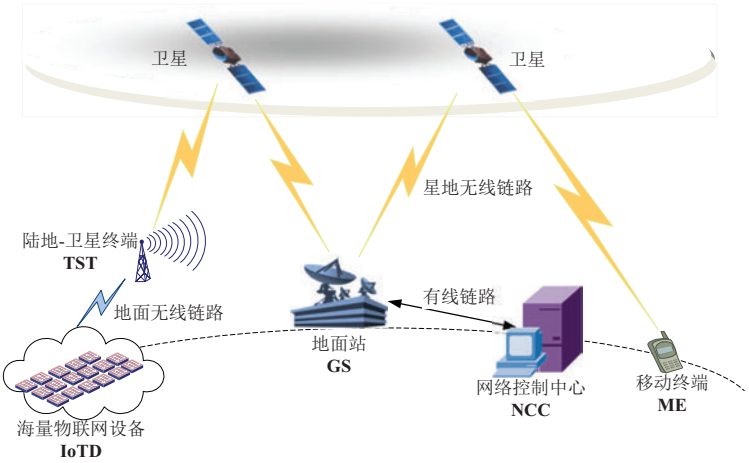


图 5.1 卫星网络架构

NCC作为陆地通信网络的重要组成部分，主要负责IoTD、ME、TST、卫星以及地面站的注册过程。

GS通过陆地通信网络连接到NCC为IoTD、ME、TST以及卫星等实体提供与地面网络通信的接口。一般来说，一个GS管辖多个卫星。

卫星代表卫星网络架构下的接入网络，主要负责转发和处理IoTD/ME和其所属GS之间的通信数据。每个卫星都会存储其所属的GS的临时身份信息。

TST是一个配有可操纵天线的专用终端[121]，部署于海量IoTD周围，可转发IoTD与卫星之间的通信数据。

IoTD是物联网业务中的设备，主要分布于远程偏远地区。IoTD通过卫星网络与陆地通信网络中的用户进行通信。每个IoTD都有一个临时设备标识。

ME代表普通用户的卫星终端，且每个ME都配备一个唯一的设备标识。

5.2.2 设计目标

设计良好的卫星网络认证方案应满足以下目标。

安全. 由于空口链路高度开放，卫星网络容易遭受各种类型的协议攻击，例如假冒攻击、中间人攻击等。因此，认证方案应该满足以下几个安全属性。

（1）相互认证

在认证过程中，UE侧与卫星网络侧都应该可以验证彼此的合法性，从而克服假冒攻击和中间人攻击。

（2）密钥协商

认证过程中UE侧与网络侧应该协商出会话密钥用以保护未来通信数据的机密性，从而克服窃听攻击。

（3）条件匿名

在认证过程中，攻击者无法获取IoTD/ME的真实身份标识，只有NCC可以获得IoTD/ME的真实身份标识。

（4） 不可链路性

攻击者无法通过认证过程中公开传输的消息区分出两条消息是否来自同一个IoTD/ME。

（5）完美前向、后向安全

即使IoTD/ME/卫星/GS的私钥暴露，攻击者也不可能获得之前或者之后的会话密钥信息。

性能. 由于卫星网络的特有属性，认证方案应该考虑以下效率需求。

（1）为提高认证成功率，应尽量减少海量IoTD并发接入时的信令开销，避免信令冲突问题。

（2）由于卫星网络与地面的超高传播时延，应尽量减少卫星网络与地面的交互次数，降低认证时延。

5.2.3　设计思路

本节的设计思路简要描述如下。首先，卫星、GS、ME、IoTD等实体在投入使用之前会在地面完成注册过程，获得身份标识以及相应的公私钥信息。随后，由于卫星与GS之间通过不安全的空口进行连接，所以为确保卫星节点与GS节点的合法性以及卫星与GS之间通信数据的机密性，每个GS与其管辖范围内的所有卫星利用注册过程获得的公私钥完成双向认证与密钥预协商过程。预协商完成之后，合法的卫星和GS之间会建立一条安全的数据通道。最后，针对接入网络实体数量的不同，提供两种差异化的接入认证服务。当海量IoTD并发激活接入卫星网络时，同一区域的海量IoTD 构成一个临时群组与接入卫星节点执行群组接入认证过程，以此克服信令冲突问题。当单个ME或者IoTD 接入卫星网络时，单个ME或者IoTD与接入卫星节点执行单个ME/IoTD的接入认证过程。在上述两个接入认证过程中，ME或者IoTD都直接与卫星节点完成双向认证，且认证过程无需依赖于地面网络节点，因此可以很大程度的降低认证时延。与此同时，为防止恶意卫星窃取通信数据，每个IoTD与GS协商通信会话密钥，卫星节点无法获知后续ME/IoTD的通信数据。

5.3 方案

本小节，详细介绍了提出的方案。首先，给出了系统设置过程；随后，描述了TST、卫星、GS、IoTD以及ME的注册过程；然后，介绍了GS与其管辖卫星间的预协商过程；接下来，分别阐述了海量IoTD的接入认证过程以及单个ME/IoTD的接入认证过程；最后，分析了方案中用到的密钥协商机制以及半聚合签名机制的正确性。

5.3.1 系统设置阶段

NCC首先选择几个相应的正整数n、q、m、β、σ以及r，并且选择五个安全的哈希函数H_1、H_2、H_3、H_4以及H_5，其中k是对称密钥的长度。随后，NCC调用算法$TrapSamp(1^n, q, m)$输出$\boldsymbol{A_N} \in Z_q^{n\times m}$和$\boldsymbol{T_N} \in Z_q^{m\times m}$分别作为它的公钥和私钥，$\boldsymbol{A_N}\boldsymbol{T_N} \equiv 0 \, mod \, q$。最后，NCC公开参数$(n, q, m, \beta, \sigma, r, k, \boldsymbol{A_N})$。表5.1 介绍了本章节用到的符号定义。

5.3.2 注册阶段

节点j，例如TST、卫星、GS、IoTD或者ME，通过安全地向NCC提供其身份标识以发起注册请求，而NCC通过安全地发出节点j的相应私钥来响应注册请求。图5.2描述了注册过程。

1. 节点j随机选择一个矩阵$\boldsymbol{S_j} \in Z_q^{n\times r}$和一个小系数噪声矩阵$\boldsymbol{X_j} \in Z_q^{m\times r}$，其中二进制矩阵$\boldsymbol{M_j} \in Z_2^{m\times r}$表示节点$j$的隐私信息，例如，节点$j$的身份标识。然后，节点$j$采用等式$\boldsymbol{C_j} \equiv \boldsymbol{A_N}^t \boldsymbol{S_j} + 2\boldsymbol{X_j} + \boldsymbol{M_j} \, mod \, q$ 加密$\boldsymbol{M_j}$。最后，节点j 发送一个注册请求消息$\boldsymbol{C_j}$给NCC。

2. NCC接收到注册请求消息后，首先按照等式$\boldsymbol{M_j}' \equiv (\boldsymbol{T_N}^t)^{-1}(\boldsymbol{T_N}^t \boldsymbol{C_j} \, mod \, q) \, mod \, 2$解密获得$\boldsymbol{M_j}'$，从$\boldsymbol{M_j}'$中解析出$id_j'$，然后检查$id_j'$的有效性，其中$(\boldsymbol{T_N}^t)^{-1}$在NCC侧只需计算一次。如果$id_j'$是有效的，NCC计算节点$j$的临时标识$\boldsymbol{tid_j}' = H_1(id_j')$，并且调用算法$ExtBasis(\boldsymbol{A_N}, \boldsymbol{tid_j}', \boldsymbol{T_N})$和算法$RandBasis(\boldsymbol{T_j}'', \sigma)$输出$\Lambda_q^{\perp}(\boldsymbol{A_N} \parallel \boldsymbol{tid_j}')$的一个随机化的基$\boldsymbol{T_j}'$。为了将基$\boldsymbol{T_j}'$安全地发送给节点$j$，NCC执行等式$\boldsymbol{C_N} = \boldsymbol{T_j}' \oplus H_2(\boldsymbol{M_j}')$。最后，NCC发送一个注册响应消息$\boldsymbol{C_N}$ 给节点j。

3. 节点j接收到注册响应消息后，首先按照等式$\boldsymbol{T_j} = \boldsymbol{C_N} \oplus H_2(\boldsymbol{M_j})$和$\boldsymbol{tid_j} = H_1(id_j)$ 得到$\boldsymbol{T_j}$以及其临时标识$\boldsymbol{tid_j}$。随后，节点j计算$\boldsymbol{A_j} = \boldsymbol{A_N} \parallel \boldsymbol{tid_j}$ 并且验证$\boldsymbol{A_j}\boldsymbol{T_j} \stackrel{?}{=} 0 \, mod \, q$。如果验证通过，节点$j$分别选择$\boldsymbol{A_j}$作为其公钥，$\boldsymbol{T_j}$ 作为其私钥。否则，节点j重新发起注册过程。

表 5.1　符号定义

符号	定义
n	一个系统安全参数
q	一个奇素数，$q \geq \beta \cdot w(\sqrt{n \log n})$
m	一个$poly(n)$有界的正整数$m \geq 8n \log q$
β	一个$SIS/ISIS$参数$\beta = poly(n)$
σ	一个高斯参数
r	一个小整数，例如$r = 1$
k	对称密钥的长度
id_j	节点j的身份标识
$\boldsymbol{tid_j}$	T节点j的临时标识，$\boldsymbol{tid_j} \in Z_q^n$
$\boldsymbol{A_N}$	NCC的公钥，$\boldsymbol{A_N} \in Z_q^{n \times m}$
$\boldsymbol{T_N}$	NCC的私钥，$\boldsymbol{T_N} \in Z_q^{m \times m}$
$\boldsymbol{A_G}$	GS的公钥，$\boldsymbol{A_G} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_G})$
$\boldsymbol{T_G}$	GS的私钥，$\boldsymbol{T_G} \in Z_q^{(m+1) \times (m+1)}$
$\boldsymbol{A_S}$	卫星的公钥，$\boldsymbol{A_S} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_S})$
$\boldsymbol{T_S}$	卫星的私钥，$\boldsymbol{T_S} \in Z_q^{(m+1) \times (m+1)}$
$\boldsymbol{A_T}$	TST的公钥，$\boldsymbol{A_T} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_T})$
$\boldsymbol{T_T}$	TST的私钥，$\boldsymbol{T_T} \in Z_q^{(m+1) \times (m+1)}$
$\boldsymbol{A_i}$	$IoTD_i$的公钥，$\boldsymbol{A_i} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_i})$
$\boldsymbol{T_i}$	$IoTD_i$的私钥，$\boldsymbol{T_i} \in Z_q^{(m+1) \times (m+1)}$
$H_1()$	$Z_2^{(m+1) \times r} \rightarrow Z_q^n$
$H_2()$	$Z_2^{(m+1) \times r} \rightarrow Z_q^{(m+1) \times (m+1)}$
$H_3()$	$Z_2^{r \times (m+1)} \rightarrow (0,1)^k$
$H_4()$	$Z_q^{n \times (m+2)} \rightarrow (0,1)^k$
$H_5()$	$Z_q^{(m+L)} \rightarrow Z_q^n$
L	IoT群组成员的个数

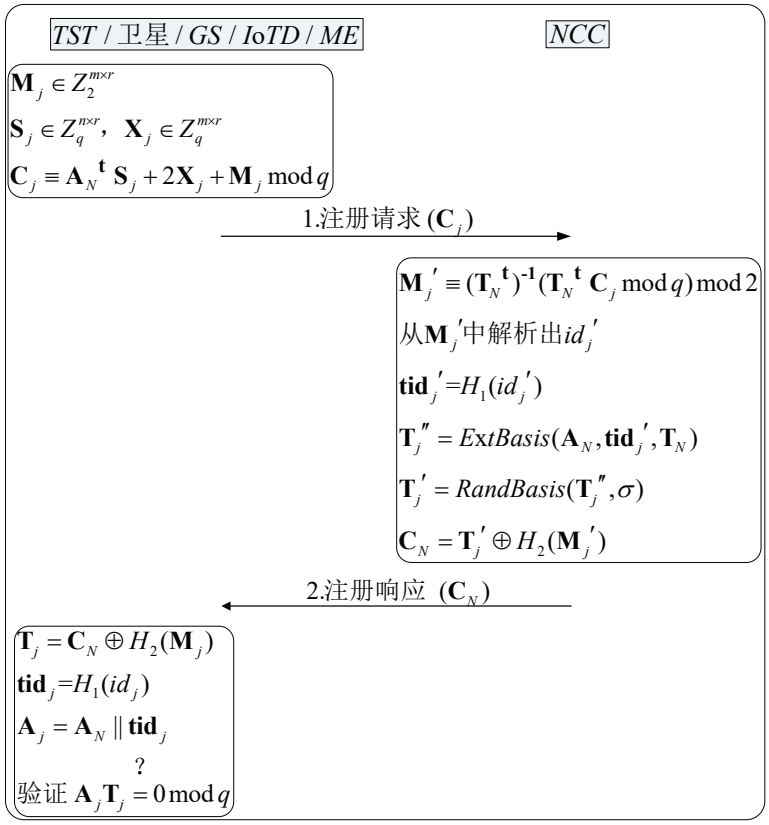


图 5.2 注册过程

5.3.3 预协商阶段

注册完成之后，如图5.3所示，每个GS和其所管辖的卫星通过验证彼此的签名完成相互认证并且利用卫星的私有信息以及GS的密钥协商参数$\boldsymbol{U_G}$安全地协商出会话密钥。

1. GS调用算法$SamplePre(\boldsymbol{T_G}, H_1(\boldsymbol{M_G}), \sigma)$生成签名$\boldsymbol{e_G}$，其中$\boldsymbol{M_G} \in Z_2^{(m+1)\times r}$代表GS的有用信息。然后，GS广播预协商请求消息$(\boldsymbol{M_G}, \boldsymbol{e_G})$给其管辖的所有卫星。

2. 卫星接收到GS广播的预协商请求消息后，首先检查$\| \boldsymbol{e_G} \| \leq \sigma\sqrt{(m+1)}$。如果成立，卫星在其数据库中搜索其所属的GS 的临时标识$\boldsymbol{tid_G}$，并且利用GS的公钥$\boldsymbol{A_G} = \boldsymbol{A_N} \| \boldsymbol{tid_G}$验证签名$\boldsymbol{A_G}\,\boldsymbol{e_G} \overset{?}{=} H_1(\boldsymbol{M_G})\, mod\, q$。如果验证成功，卫星随机选择一个矩阵$\boldsymbol{R_S} \in Z_q^{n\times r}$ 以及一个小系数噪声矩阵$\boldsymbol{X_S} \in Z_q^{(m+1)\times r}$，按照等式$\boldsymbol{C_S} \equiv \boldsymbol{A_G}{}^t\,\boldsymbol{R_S} + 2\boldsymbol{X_S} + \boldsymbol{M_S}\, mod\, q$加密隐私消息$\boldsymbol{M_S} \in Z_2^{(m+1)\times r}$，其中$\boldsymbol{M_S}$代表卫星需要传输给GS的必要信息。另外，卫星调用算法$SamplePre(\boldsymbol{T_S}, H_1(\boldsymbol{M_S}), \sigma)$ 生成签名$\boldsymbol{e_S}$。最后，卫星传输一个预协商响应消息$(\boldsymbol{C_S}, \boldsymbol{e_S})$给GS。

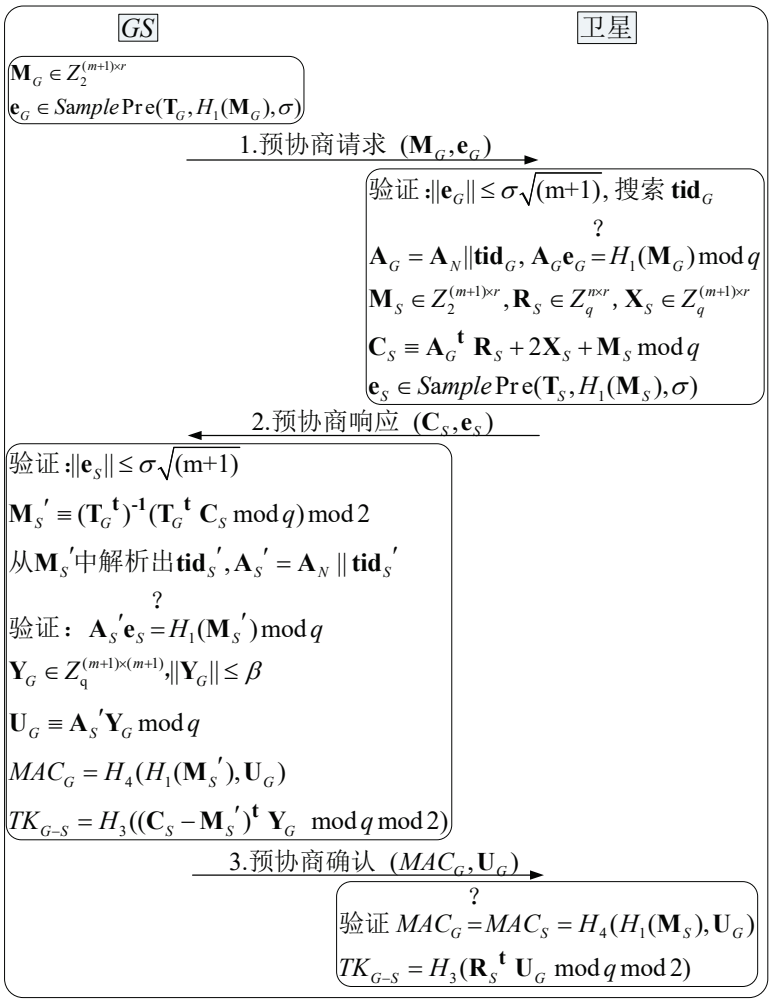


图 5.3　预协商过程

3. GS接收到预协商响应消息后，首先验证等式$\| \boldsymbol{e_S} \| \le \sigma\sqrt{(m+1)}$。如果验证成功，GS获取卫星的隐私信息$\boldsymbol{M_S'} \equiv (\boldsymbol{T_G}^t)^{-1}(\boldsymbol{T_G}^t\,\boldsymbol{C_S} \bmod q) \bmod 2$，从$\boldsymbol{M_S'}$中解析出临时标识$\boldsymbol{tid_S'}$，然后获取卫星的公钥$\boldsymbol{A_S'} = \boldsymbol{A_N} \| \boldsymbol{tid_S'}$。随后，GS通过检查等式$\boldsymbol{A_S'e_S} \stackrel{?}{=} H_1(\boldsymbol{M_S'}) \bmod q$认证卫星。如果认证成功，GS随机选择一个矩阵$\boldsymbol{Y_G} \in Z_q^{(m+1)\times(m+1)}$，满足$\| \boldsymbol{Y_G} \| \le \beta$。然后，GS计算会话密钥协商参数$\boldsymbol{U_G} \equiv \boldsymbol{A_S'}\,\boldsymbol{Y_G} \bmod q$以及用于和卫星安全通信的会话密钥$TK_{G-S} = H_3((\boldsymbol{C_S} - \boldsymbol{M_S'})^t\,\boldsymbol{Y_G} \bmod q \bmod 2)$。随后，GS计算$MAC_G = H_4(H_1(\boldsymbol{M_S'}), \boldsymbol{U_G})$。最后，GS发送一个预协商确认消息$(MAC_G, \boldsymbol{U_G})$给卫星。

4. 卫星接收到预协商确认消息后，通过检查等式$MAC_G \stackrel{?}{=} MAC_S = H_4(H_1(\boldsymbol{M_S}), \boldsymbol{U_G})$认证GS。如果认证成功，卫星计算用于和GS安全通信的会话密钥$TK_{G-S} = H_3((\boldsymbol{R_S}^t\,\boldsymbol{U_G} \bmod q \bmod 2)$。最后，卫星存储数据$\boldsymbol{U_G}$用于未来认证过程中的密钥协商。

5.3.4 认证阶段

1. 海量IoTD的接入认证阶段

当海量IoTD请求接入卫星网络时，如图5.4所示，他们构成一个临时的IoT群组执行认证过程。假设群成员的个数为L。在此阶段，目标卫星通过验证单一半聚合签名和半聚合签名机制的辅助信息认证IoT群组，而每个IoTD通过检查哈希值认证卫星。与此同时，每个IoTD与GS基于IoTD的隐私信息以及GS的密钥协商参数协商出会话密钥。具体过程如下。

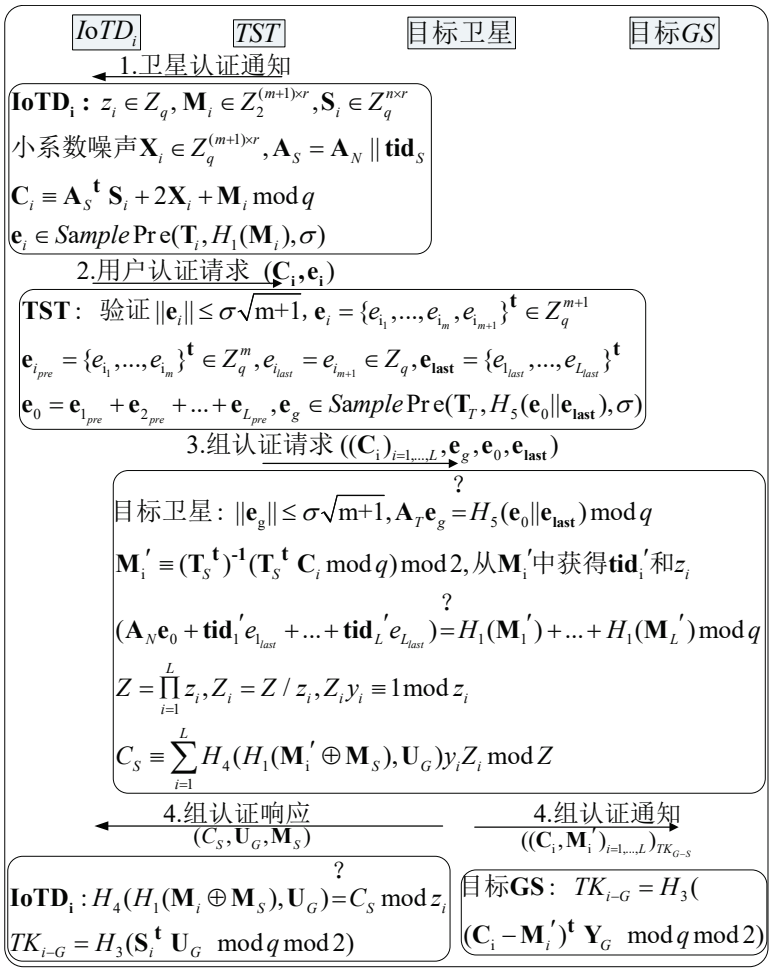


图 5.4 海量IoTD的接入认证过程

(1) TST监测到新卫星出现后广播一个卫星认证通知消息并且启动一个时延定时器。

(2) 每个需要接入卫星网络的$IoTD_i$接收到卫星认证通知消息后，随机选择一个素数$z_i \in Z_q$，一个矩阵$\boldsymbol{S_i} \in Z_q^{n\times r}$以及一个小系数噪声矩阵$\boldsymbol{X_i} \in Z_q^{(m+1)\times r}$。$IoTD_i$的隐私信息表示为一个二进制矩阵$\boldsymbol{M_i} \in Z_2^{(m+1)\times r}$，具体内容包括$z_i$以

及其他用于认证的必要信息，例如临时标识$\boldsymbol{tid}_i$。然后，$IoTD_i$借助于卫星的公钥$\boldsymbol{A_S} = \boldsymbol{A_N} \parallel \boldsymbol{tid_S}$采用等式$\boldsymbol{C_i} \equiv \boldsymbol{A_S}^t \boldsymbol{S_i} + 2\boldsymbol{X_i} + \boldsymbol{M_i} \bmod q$加密$\boldsymbol{M_i}$。最后，$IoTD_i$调用算法$SamplePre(\boldsymbol{T_i}, H_1(\boldsymbol{M_i}), \sigma)$生成消息$\boldsymbol{M_i}$一个签名$\boldsymbol{e}_i$。最后，$IoTD_i$发送用户认证请求消息$(\boldsymbol{C_i}, \boldsymbol{e}_i)$给TST。

(3) 当计时器的时间戳到达时，TST首先验证所有接收到的签名$\boldsymbol{e}_i$是否满足$\| \boldsymbol{e_i} \| \leq \sigma\sqrt{m+1}$，$i = 1, ..., L$。如果是，TST按照如下步骤执行半聚合签名机制。首先，由于$\boldsymbol{e_i} = \{e_{i_1}, ..., e_{i_m}, e_{i_{m+1}}\}^t$是$(m+1)$维向量，令$\boldsymbol{e_{i_{pre}}} = \{e_{i_1}, ..., e_{i_m}\}^t$，$e_{i_{last}} = e_{i_{m+1}}$，$\boldsymbol{e_{last}} = \{e_{1_{last}}, ..., e_{L_{last}}\}^t$。然后，TST按照等式$\boldsymbol{e_0} = \boldsymbol{e_{1_{pre}}} + ... + \boldsymbol{e_{L_{pre}}}$聚合所有的$(\boldsymbol{e_{i_{pre}}})_{i=1,...,L}$为一个$\boldsymbol{e_0}$。随后，TST调用算法$SamplePre(\boldsymbol{T_T}, H_5(\boldsymbol{e_0}||\boldsymbol{e_{last}}), \sigma)$生成$\boldsymbol{e_g}$并且发送一个群组认证请求消息给目标卫星，其中请求消息内容包括半聚合签名$\boldsymbol{e_0}$、$\boldsymbol{e_g}$、密文$(\boldsymbol{C_i})_{i=1,...,L}$以及一些签名辅助信息$\boldsymbol{e_{last}}$。

(4) 目标卫星接收到群组认证请求消息后，首先验证等式$\| \boldsymbol{e_g} \| \leq \sigma\sqrt{m+1}$和$\boldsymbol{A_T e_g} \stackrel{?}{=} H_5(\boldsymbol{e_0}||\boldsymbol{e_{last}}) \bmod q$。如果验证成功，目标卫星通过等式$\boldsymbol{M_i}' \equiv (\boldsymbol{T_S}^t)^{-1} (\boldsymbol{T_S}^t \boldsymbol{C_i} \bmod q) \bmod 2$计算每个$IoTD_i$的隐私信息，其中$(\boldsymbol{T_S}^t)^{-1}$只需在认证过程之前计算一次。然后，目标卫星从$\boldsymbol{M_i}'$中获得每个$IoTD_i$的临时标识$\boldsymbol{tid_i}'$和$z_i$。进而，目标卫星按照等式$\boldsymbol{A}_N \boldsymbol{e_0} + \boldsymbol{tid_1}' e_{1_{last}} + ... + \boldsymbol{tid_L}' e_{L_{last}} \stackrel{?}{=} H_1(\boldsymbol{M}_1') + ... + H_1(\boldsymbol{M}_L') \bmod q$验证签名。如果验证成功，目标卫星采用中国剩余定理[122]产生哈希值，具体如下。

$$Z = \prod_{i=1}^{L} z_i, Z_i = Z/z_i, Z_i\, y_i \equiv 1 mod\, z_i$$

$$C_S \equiv \sum_{i=1}^{L} H_4(H_1(\boldsymbol{M_i}' \oplus \boldsymbol{M_S}), \boldsymbol{U_G}) y_i\, Z_i \bmod Z$$

最后，目标卫星发送一个群组认证响应消息$(C_S, \boldsymbol{U_G}, \boldsymbol{M_S})$给IoT群组，其中$\boldsymbol{M_S}$是用于通信的必要信息，而$\boldsymbol{U_G}$是在预协商过程中从GS获得的。与此同时，目标卫星采用密钥TK_{G-S}加密参数$(\boldsymbol{C_i}, \boldsymbol{M_i}')_{i=1,...,L}$，并且将密文传输给GS。

(5) $IoTD_i$接收到群组认证响应消息后，首先验证等式$H_4(H_1(\boldsymbol{M_i} \oplus \boldsymbol{M_S}), \boldsymbol{U_G}) \stackrel{?}{=} C_S \bmod z_i$。如果验证通过，$IoTD_i$计算会话密钥$TK_{i-G} = H_3(\boldsymbol{S_i}^t \boldsymbol{U_G} \bmod q \bmod 2)$。

(6) 目标GS接收到群组认证通知消息后，计算用于和每个$IoTD_i$安全通信的会话密钥$TK_{i-G} = H_3((\boldsymbol{C_i} - \boldsymbol{M_i}')^t \boldsymbol{Y_G} \bmod q \bmod 2)$，其中$\boldsymbol{Y_G}$是在预协商阶段产生的。

执行完上述步骤之后，每个$IoTD_i$和GS建立了一条安全的数据通道。

2. 单个ME/IoTD的接入认证阶段

当一个普通的ME或者单一的IoTD (统一表示为$IoTD_i$)请求接入卫星，它执行图5.5中的认证过程。在此过程中，目标卫星通过检验$IoTD_i$的签名值认证$IoTD_i$，而$IoTD_i$通过检查哈希值认证目标卫星。与此同时，每个$IoTD_i$和GS协商出一个会话密钥。具体描述如下。

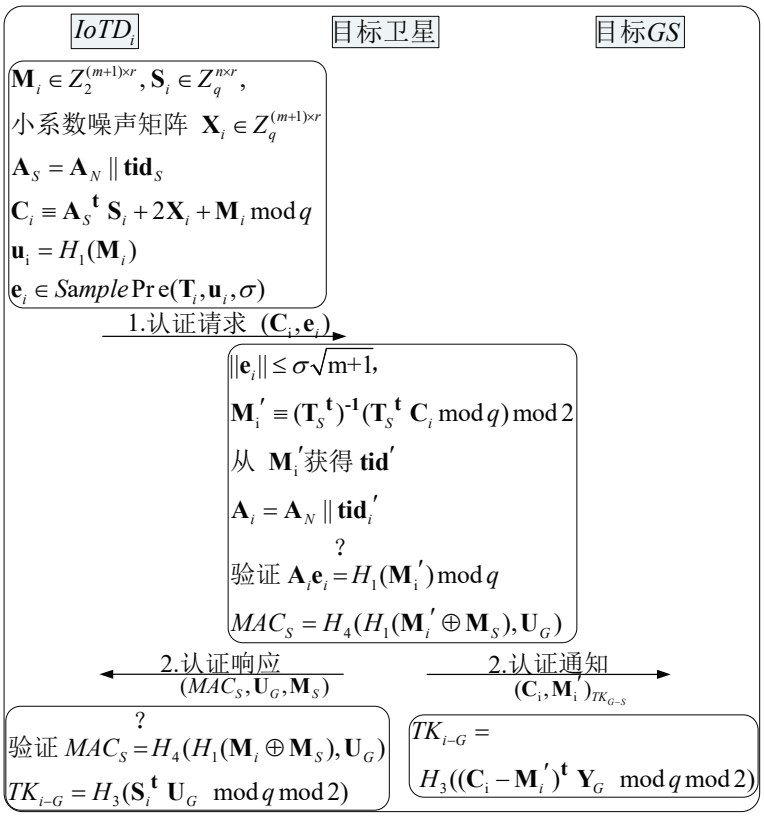


图 5.5 单个ME/IoTD的接入认证过程

(1) 当$IoTD_i$请求接入卫星，它执行与海量IoTD的接入认证过程中步骤(2)相同的操作。最后，$IoTD_i$直接发送一个认证请求消息$(\boldsymbol{C_i}, \boldsymbol{e_i})$给目标卫星。

(2) 目标卫星接收到认证请求消息后，首先验证等式$\| \boldsymbol{e_i} \| \leq \sigma\sqrt{m+1}$是否成立。如果成立，目标卫星同样按照海量IoTD的接入认证过程中步骤(4)相同的操作计算出隐私信息$\boldsymbol{M_i'}$，并且从$\boldsymbol{M_i'}$中获取临时标识$\boldsymbol{tid_i'}$。目标卫星计算$IoTD_i$的公钥$\boldsymbol{A_i} = \boldsymbol{A_N} \| \boldsymbol{tid_i'}$。然后，目标卫星通过检查等式$\boldsymbol{A_i}\,\boldsymbol{e_i} \stackrel{?}{=} H_1(\boldsymbol{M_i'})\,mod\,q$是否成立认证$IoTD_i$。如果成功认证，目标卫星计算哈希值$MAC_S = H_4(H_1(\boldsymbol{M_i'} \oplus \boldsymbol{M_S}), \boldsymbol{U_G})$，并且发送认证响应消息$MAC_S$，密钥协商参数$\boldsymbol{U_G}$以及目标卫星的有用信息$\boldsymbol{M_S}$给$IoTD_i$。同时，目标卫星发送一个认证通知消息给目标GS，其中消息内容包括加密后的$(\boldsymbol{C_i}, \boldsymbol{M_i'})$。

(3) $IoTD_i$接收到认证响应消息后，通过等式$MAC_S \stackrel{?}{=} H_4(H_1(\boldsymbol{M_i} \oplus \boldsymbol{M_S}), \boldsymbol{U_G})$认证目标卫星。如果认证成功，$IoTD_i$计算会话密钥$TK_{i-G} = H_3(\boldsymbol{S_i}^t \boldsymbol{U_G} \, mod q \, mod 2)$。与此同时，目标GS接收到认证通知消息后，直接计算与每个$IoTD_i$安全通信的会话密钥$TK_{i-G} = H_3((\boldsymbol{C_i} - \boldsymbol{M_i}')^t \boldsymbol{Y_G} \, mod q \, mod 2)$。

执行完上述接入认证过程之后，每个$IoTD_i$与目标GS之间建立了一条安全的数据通道。

5.3.5　正确性评估

（1）会话密钥协商机制的正确性:

基于Gentry的加密机制[72], 选择合适的参数使得等式$2\boldsymbol{X_i}^t \boldsymbol{Y_G} < q$成立，进而$2\boldsymbol{X_i}^t \boldsymbol{Y_G} \equiv 0 \, mod \, q \, mod \, 2$。因此，可以得到：

$$\begin{aligned} TK_{i-G} &= H_3((\boldsymbol{C_i} - \boldsymbol{M_i}')^t \boldsymbol{Y_G} \, mod \, q \, mod \, 2) \\ &= H_3(((\boldsymbol{A_S}^t \boldsymbol{S_i} + 2\boldsymbol{X_i})^t \boldsymbol{Y_G}) \, mod \, q \, mod \, 2) \\ &= H_3(\boldsymbol{S_i}^t \boldsymbol{A_S} \, \boldsymbol{Y_G} \, mod \, q \, mod \, 2) \\ &= H_3(\boldsymbol{S_i}^t \boldsymbol{U_G} \, mod \, q \, mod \, 2). \end{aligned}$$

（2）半聚合签名机制的正确性:

$$\begin{aligned} & \boldsymbol{A}_N \boldsymbol{e_0} + \boldsymbol{tid_1}' \, e_{1_{last}} + ... + \boldsymbol{tid_L}' \, e_{L_{last}} \\ & \equiv \boldsymbol{A}_N(\boldsymbol{e_{1_{pre}}} + ... + \boldsymbol{e_{L_{pre}}}) + \boldsymbol{tid_1}' e_{1_{last}} + ... + \boldsymbol{tid_L}' e_{L_{last}} \\ & \equiv (\boldsymbol{A}_N \boldsymbol{e_{1_{pre}}} + \boldsymbol{tid_1}' e_{1_{last}}) + ... + (\boldsymbol{A}_N \boldsymbol{e_{L_{pre}}} + \boldsymbol{tid_L}' e_{L_{last}}) \\ & \equiv (\boldsymbol{A}_N || \boldsymbol{tid_1}') \boldsymbol{e_1} + ... + (\boldsymbol{A}_N || \boldsymbol{tid_L}') \boldsymbol{e_L} \\ & \equiv \boldsymbol{A}_1 \boldsymbol{e_1} + ... + \boldsymbol{A}_L \boldsymbol{e_L} \\ & \equiv H_1(\boldsymbol{M}_1') + ... + H_1(\boldsymbol{M}_L') \ mod \, q. \end{aligned}$$

5.4　安全评估

本节，采用可证明安全分析、BAN逻辑以及非形式化安全分析证明了提出方案的安全性。

5.4.1　可证明安全分析

本小节，采用了文献[68–70]中的可证明安全分析模型证明了提出方案的安全性。由于提出方案中采用的基本签名机制已经被证明满足选择消息攻击下强不可伪造性（strongly UnForgeable Chosen Message Attack，sUF-CMA）[69]，这里只考虑海量IoTD的接入认证过程中采用的半聚合签名机制的安全性。

定理. 在小整数解的困难问题假设下，包含在半聚合签名中的基本签名是sUF-CMA安全。

证明. 如果攻击者$\mathcal{A}$伪造了一个有效的半聚合签名$(\boldsymbol{e_g^*}, \boldsymbol{e_0^*}, \boldsymbol{e_{last}^*}, (\boldsymbol{C_i^*})_{i=1,...,v})$ 中的基本签名$\boldsymbol{e_x^*}$或者直接伪造了一个半聚合签名$(\boldsymbol{e_g^*}, \boldsymbol{e_0^*}, \boldsymbol{e_{last}^*}, (\boldsymbol{C_i^*})_{i=1,...,v})$，就可以构造一个仿真器$\mathcal{D}$利用$\mathcal{A}$解决$SIS_{q,m,2\sigma\sqrt{m+1}}$。

初始化: $\mathcal{D}$执行如下步骤。

(1) $\mathcal{D}$按照系统设置阶段定义$\boldsymbol{A_N} \in Z_q^{n\times m}$和$\boldsymbol{T_N} \in Z_q^{m\times m}$分别作为系统公钥和私钥，并且公开参数$(n, q, m, \beta, \sigma, r, k, \boldsymbol{A_N})$。

(2) $\mathcal{D}$ 分别生成目标卫星和TST的公钥为$\boldsymbol{A_S} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_S}) \in Z_q^{n\times(m+1)}$和$\boldsymbol{A_T} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_T}) \in Z_q^{n\times(m+1)}$，其中$tid_S$和$tid_T$分别是目标卫星和TST的临时标识。

(3) $\mathcal{D}$公开$(\boldsymbol{A_N}, \boldsymbol{A_T})$。

攻击: $\mathcal{A}$可以执行H_1询问、H_5询问、$sign$询问、$semi-aggregated\ sign$询问以及$encryption$ 询问。不失一般性，假设在执行$sign$ 询问之前，$\mathcal{A}$一定询问过H_1或者H_5。另外，假设$\mathcal{A}$是通过询问$encryption$而获得关于$\boldsymbol{M_i}$的密文。

- H_1 询问: $\mathcal{A}$对消息$\boldsymbol{M_i}$执行H_1询问。$\mathcal{D}$从$\boldsymbol{M_i}$中解析出$\boldsymbol{tid_i}$ ，进而生成相应的公钥$\boldsymbol{A_i} = (\boldsymbol{A_N} \parallel \boldsymbol{tid_i})$，其中$\boldsymbol{tid_i}$ 代表$IoTD_i$的临时标识。$\mathcal{D}$持有一个初始为空的列表$\mathcal{L}_{H_1}$。如果记录$(\boldsymbol{M_i}, *, *, \boldsymbol{u_i^{\mathcal{L}_{H_1}}})$在列表$\mathcal{L}_{H_1}$中存在，$\mathcal{D}$ 返回$\boldsymbol{u_i^{\mathcal{L}_{H_1}}}$ 给$\mathcal{A}$。否则，$\mathcal{D}$生成$\boldsymbol{e_i^{\mathcal{L}_{H_1}}} \leftarrow SampleDom(\boldsymbol{A_i}, \sigma)$。然后,$\mathcal{D}$计算$\boldsymbol{u_i^{\mathcal{L}_{H_1}}} \equiv \boldsymbol{A_i}\, \boldsymbol{e_i^{\mathcal{L}_{H_1}}} \bmod q$，添加$(\boldsymbol{M_i}, \boldsymbol{e_i^{\mathcal{L}_{H_1}}}, \psi_i^{\mathcal{L}_{H_1}} = 0, \boldsymbol{u_i^{\mathcal{L}_{H_1}}})$到列表$\mathcal{L}_{H_1}$中，然后返回$\boldsymbol{u_i^{\mathcal{L}_{H_1}}}$给$\mathcal{A}$。

- H_5 询问: $\mathcal{A}$对消息$\boldsymbol{M_t}$执行H_5询问。$\mathcal{D}$维持一个初始为空的列表$\mathcal{L}_{H_5}$。如果记录$(\boldsymbol{M_t}, *, *, \boldsymbol{u_t^{\mathcal{L}_{H_5}}})$在列表$\mathcal{L}_{H_5}$中存在，$\mathcal{D}$返回$\boldsymbol{u_t^{\mathcal{L}_{H_5}}}$ 给$\mathcal{A}$。否则$\mathcal{D}$选择$\boldsymbol{e_t^{\mathcal{L}_{H_5}}} \leftarrow SampleDom(\boldsymbol{A_T}, \sigma)$。然后，$\mathcal{D}$计算$\boldsymbol{u_t^{\mathcal{L}_{H_5}}} \equiv \boldsymbol{A_T}\, \boldsymbol{e_t^{\mathcal{L}_{H_5}}} \bmod q$,，添加$(\boldsymbol{M_t}, \boldsymbol{e_t^{\mathcal{L}_{H_5}}}, \psi_t^{\mathcal{L}_{H_5}} = 0, \boldsymbol{u_t^{\mathcal{L}_{H_5}}})$到列表$\mathcal{L}_{H_5}$中，然后返回$\boldsymbol{u_t^{\mathcal{L}_{H_5}}}$给$\mathcal{A}$。

- $Sign$ 询问: $\mathcal{A}$请求$\mathcal{D}$生成消息$\boldsymbol{M_j}$以及相应公钥$\boldsymbol{A_j} \in Z_q^{n\times(m+1)}$的签名。如果$\boldsymbol{A_j} = \boldsymbol{A_T}$，$\mathcal{D}$搜索列表$\mathcal{L}_{H_5}$并返回$\boldsymbol{e_j^{\mathcal{L}_{H_5}}}$。否则，如果$\boldsymbol{A_j} \neq \boldsymbol{A_T}$且$\boldsymbol{A_j} \equiv (\boldsymbol{A_N} \parallel \boldsymbol{tid_j})$，其中$\boldsymbol{tid_j}$是从$\boldsymbol{M_j}$中获得，$\mathcal{D}$搜索列表$\mathcal{L}_{H_1}$并返回$\boldsymbol{e_j^{\mathcal{L}_{H_1}}}$。最后，$\mathcal{D}$设置列表$\mathcal{L}_{H_1}$或$\mathcal{L}_{H_5}$中相应的$\psi_j^{\mathcal{L}_{H_1}} = 1$或者$\psi_j^{\mathcal{L}_{H_5}} = 1$。

- $Semi-aggregated\,sign$ 询问: $\mathcal{A}$请求$\mathcal{D}$生成关于多个基本签名消息$(\boldsymbol{e_1}, \boldsymbol{e_2}, ..., \boldsymbol{e_v})$的半聚合签名。$\mathcal{D}$首先验证$\parallel \boldsymbol{e_i} \parallel \leq \sigma\sqrt{m+1}$，$i = 1, ..., v$。然后$\mathcal{D}$令$\boldsymbol{e_i} = \{e_{i_1}, ..., e_{i_m}, e_{i_{m+1}}\}^t$，$\boldsymbol{e_{i_{pre}}} = \{e_{i_1}, ..., e_{i_m}\}^t$，$e_{i_{last}} = e_{i_{m+1}}$，$\boldsymbol{e_{last}} = \{e_{1_{last}}, ..., e_{v_{last}}\}^t$

并且计算$\boldsymbol{e_0} = \boldsymbol{e_{1_{pre}}} + ... + \boldsymbol{e_{v_{pre}}}$。最后，$\mathcal{D}$对$\boldsymbol{e_0}||\boldsymbol{e_{last}}$执行$sign$询问获取$\boldsymbol{e_g}$，并且返回$\boldsymbol{e_g}, \boldsymbol{e_0}$以及辅助信息$\boldsymbol{e_{last}}$。

- *Encryption* 询问: $\mathcal{A}$请求$\mathcal{D}$加密消息$\boldsymbol{M_i}$。如果记录$(\boldsymbol{M_i}, \boldsymbol{C_i^{\mathcal{L}_T}})$在列表$\mathcal{L}_T$中存在，$\mathcal{D}$返回$\boldsymbol{C_i^{\mathcal{L}_T}}$。否则，$\mathcal{D}$随机选择两个矩阵$\boldsymbol{X_i} \in Z_q^{(m+1)\times r}$和$\boldsymbol{S_i} \in Z_q^{n\times r}$，并且计算$\boldsymbol{C_i^{\mathcal{L}_T}} \equiv \boldsymbol{A_S}^t \boldsymbol{S_i} + 2\boldsymbol{X_i} + \boldsymbol{M_i} \bmod q$。最后，$\mathcal{D}$返回$\boldsymbol{C_i^{\mathcal{L}_T}}$并且添加$(\boldsymbol{M_i}, \boldsymbol{C_i^{\mathcal{L}_T}})$至列表$\mathcal{L}_T$.

伪造： $\mathcal{A}$输出半聚合签名消息$(\boldsymbol{e_g^*}, \boldsymbol{e_0^*}, \boldsymbol{e_{last}^*}, (\boldsymbol{C_i^*})_{i=1,...,v})$。不失一般性，假设在输出伪造消息之前，$\mathcal{A}$对所有消息执行过$H_1$或$H_5$询问。

$\mathcal{D}$接收到伪造的消息$(\boldsymbol{e_g^*}, \boldsymbol{e_0^*}, \boldsymbol{e_{last}^*}, (\boldsymbol{C_i^*})_{i=1,...,v})$后，在列表$\mathcal{L}_{H_5}$中搜索记录$(\boldsymbol{e_0^*}||\boldsymbol{e_{last}^*}, \boldsymbol{e_t^{\mathcal{L}_{H_5}}}, \psi_t^{\mathcal{L}_{H_5}}, \boldsymbol{u_t^{\mathcal{L}_{H_5}}})$，并且验证$\| \boldsymbol{e_g^*} \| \leq \sigma\sqrt{m+1}$和$\boldsymbol{A_T e_g^*} \stackrel{?}{=} \boldsymbol{u_t^{\mathcal{L}_{H_5}}} \bmod q$。如果验证成功，$\mathcal{D}$在列表$\mathcal{L}_T$中寻找相应的$(\boldsymbol{M_i^{\mathcal{L}_T}})_{i=1,...,v}$。随后，$\mathcal{D}$在列表$\mathcal{L}_{H_1}$中搜索记录$(\boldsymbol{M_i^{\mathcal{L}_T}}, \boldsymbol{e_i^{\mathcal{L}_{H_1}}}, \psi_i^{\mathcal{L}_{H_1}}, \boldsymbol{u_i^{\mathcal{L}_{H_1}}})$，并且验证$\boldsymbol{A}_N\, \boldsymbol{e_0^*} + \boldsymbol{tid_1}\, e_{1_{last}}^* + ... + \boldsymbol{tid_v}\, e_{v_{last}}^* \stackrel{?}{=} \boldsymbol{u_1^{\mathcal{L}_{H_1}}} + ... + \boldsymbol{u_v^{\mathcal{L}_{H_1}}} \bmod q$，其中$\boldsymbol{tid_i}$和$e_{i_{last}}^*$分别从$\boldsymbol{M_i^{\mathcal{L}_T}}$和$\boldsymbol{e_{last}^*}$中获得。如果所有的验证成功，考虑以下三种情形。

Case 1 如果$\psi_t^{\mathcal{L}_{H_5}} = 0$，由于$\mathcal{A}$已经执行过$H_5$询问，可以得到$\boldsymbol{A_T e_t^{\mathcal{L}_{H_5}}} \equiv \boldsymbol{u_t^{\mathcal{L}_{H_5}}} \bmod q$，$\boldsymbol{A_T e_g^*} \equiv \boldsymbol{u_t^{\mathcal{L}_{H_5}}} \bmod q$且$\boldsymbol{A_T}(\boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}}) \equiv \boldsymbol{0} \bmod q$。根据三角不等式定理，由于$\| \boldsymbol{e_g^*} \| \leq \sigma\sqrt{m+1}$且$\| \boldsymbol{e_t^{\mathcal{L}_{H_5}}} \| \leq \sigma\sqrt{m+1}$，有$\| \boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}} \| \leq 2\sigma\sqrt{m+1}$。另外，根据哈希函数的前象最小熵性质[69]，$\boldsymbol{e_t^{\mathcal{L}_{H_5}}} \neq \boldsymbol{e_g^*}$以压倒性的概率$1 - 2^{-w(logn)}$发生。因此，$\boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}}$以压倒性的概率是$SIS_{q,m,2\sigma\sqrt{m+1}}$的解。

Case 2 如果$\psi_t^{\mathcal{L}_{H_5}} = 1$且$\boldsymbol{e_g^*} \neq \boldsymbol{e_t^{\mathcal{L}_{H_5}}}$，类似地，有$\boldsymbol{A_T}(\boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}}) \equiv \boldsymbol{0} \bmod q$且$\| \boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}} \| \leq 2\sigma\sqrt{m+1}$。明显地，$\boldsymbol{e_g^*} - \boldsymbol{e_t^{\mathcal{L}_{H_5}}}$是$SIS_{q,m,2\sigma\sqrt{m+1}}$的解。

Case 3 如果$\psi_t^{\mathcal{L}_{H_5}} = 1$且$\boldsymbol{e_g^*} = \boldsymbol{e_t^{\mathcal{L}_{H_5}}}$，我们认为$\mathcal{A}$伪造了一个关于消息$\boldsymbol{M_x^{\mathcal{L}_T}}$的基本签名$\boldsymbol{e_x^*}$并执行了对这些基本签名$(\boldsymbol{e_1}, \boldsymbol{...e_x^*}, \boldsymbol{..., e_v})$的$semi-aggregated\ sign$询问获得了$(\boldsymbol{e_g^*}, \boldsymbol{e_T^*}, (\boldsymbol{C_i^*}, e_{i_{last}}^*)_{i=1,...,v})$，其中$(\boldsymbol{e_i})_{i=1,...,v,i\neq x}$来自$sign$询问。进而，$\mathcal{D}$在列表$\mathcal{L}_{H_1}$中搜索记录$(\boldsymbol{M_x^{\mathcal{L}_T}}, \boldsymbol{e_x^{\mathcal{L}_{H_1}}}, \psi_x^{\mathcal{L}_{H_1}}, \boldsymbol{u_x^{\mathcal{L}_{H_1}}})$并且考虑如下两种情形：1)如果$\psi_x^{\mathcal{L}_{H_1}} = 1$，$\mathcal{A}$针对消息$\boldsymbol{M_x^{\mathcal{L}_T}}$已经执行过程$sign$询问并且获得了$\boldsymbol{e_x^{\mathcal{L}_{H_1}}}$。因为此消息被认为是伪造的，可以得到$\boldsymbol{e_x^{\mathcal{L}_{H_1}}} \neq \boldsymbol{e_x^*}$。2) 如果$\psi_x^{\mathcal{L}_{H_1}} = 0$，根据哈希函数的前象最小熵特性，$\boldsymbol{e_x^{\mathcal{L}_{H_1}}} \neq \boldsymbol{e_x^*}$以压倒性的优势$1 - 2^{-w(logn)}$发生。另外。由于

$$
\begin{aligned}
&\boldsymbol{A}_N\, \boldsymbol{e_0^*} + \boldsymbol{tid_1}\, e_{1_{last}}^* + ... + \boldsymbol{tid_v}\, e_{v_{last}}^* \\
&\equiv (\boldsymbol{A}_N \boldsymbol{e_{1_{pre}}} + \boldsymbol{tid_1}\, e_{1_{last}}^*) + ... + (\boldsymbol{A}_N \boldsymbol{e_{v_{pre}}} + \boldsymbol{tid_v}\, e_{v_{last}}^*) \\
&\equiv \boldsymbol{A}_1 \boldsymbol{e_1^{\mathcal{L}_{H_1}}} + ... + \boldsymbol{A}_x \boldsymbol{e_x^*} + ... + \boldsymbol{A}_v \boldsymbol{e_v^{\mathcal{L}_{H_1}}} \\
&\equiv \boldsymbol{u_1^{\mathcal{L}_{H_1}}} + ... + \boldsymbol{u_x^{\mathcal{L}_{H_1}}} + ... + \boldsymbol{u_v^{\mathcal{L}_{H_1}}} \bmod q.
\end{aligned}
$$

且$\boldsymbol{e}_i^{\mathcal{L}_{H_1}} = \boldsymbol{e}_i$，$\boldsymbol{A}_i\,\boldsymbol{e}_i^{\mathcal{L}_H} \equiv \boldsymbol{u}_i^{\mathcal{L}_H} mod\, q$，$i = 1, ..., v, i \neq x$，因此可以得到$\boldsymbol{A}_x\,\boldsymbol{e}_x^* \equiv \boldsymbol{u}_x^{\mathcal{L}_{H_1}} mod\, q$。由于$\boldsymbol{A}_x\,\boldsymbol{e}_x^{\mathcal{L}_{H_1}} \equiv \boldsymbol{u}_x^{\mathcal{L}_{H_1}} mod\, q$，$\| \boldsymbol{e}_x^{\mathcal{L}_{H_1}} \| \leq \sigma\sqrt{m+1}$且$\| \boldsymbol{e}_x^* \| \leq \sigma\sqrt{m+1}$，基于三角不等式和$\boldsymbol{A}_x\,(\boldsymbol{e}_x^{\mathcal{L}_{H_1}} - \boldsymbol{e}_x^*) \equiv \boldsymbol{0}\, mod\, q$，可以得到$\| \boldsymbol{e}_x^{\mathcal{L}_{H_1}} - \boldsymbol{e}_x^* \| \leq 2\sigma\sqrt{m+1}$。因此，$(\boldsymbol{e}_x^{\mathcal{L}_{H_1}} - \boldsymbol{e}_x^*)$ 以不可忽略的概率是$SIS_{q,m,2\sigma\sqrt{m+1}}$ 解。

综上所述, 如果$\mathcal{A}$成功伪造了一个半聚合签名机制中的基本签名或者直接伪造了一个半聚合签名，$\mathcal{D}$就能以不可忽略的概率解决$SIS_{q,m,2\sigma\sqrt{m+1}}$，这显然与小整数解假设相矛盾。

5.4.2 逻辑分析工具：BAN

本小节，采用逻辑分析工具BAN证明提出的单个ME/IoTD的接入认证协议满足卫星与$IoTD_i$ 之间的相互认证以及$IoTD_i$与目标GS之间的密钥协商。为了叙述简便起见，采用S表示卫星，G表示目标GS。

提出的单个ME/IoTD的接入认证协议中所涉及的消息可以简化如下。

M1. $IoTD_i \rightarrow S : (\boldsymbol{C_i}, \boldsymbol{e}_i)$

M2. $S \rightarrow IoTD_i : (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

M3. $S \rightarrow G : (\{\boldsymbol{C_i}, \boldsymbol{M_i}'\}_{TK_{G-S}})$

单个ME/IoTD的接入认证协议的安全目标是实现相互认证与密钥协商，表述如下。

G1. $S \mid\equiv (\boldsymbol{C_i}, \boldsymbol{e}_i)$

G2. $IoTD_i \mid\equiv S \mid\equiv \boldsymbol{M_i}'$

G3. $IoTD_i \mid\equiv TK_{i-G}$

G4. $G \mid\equiv TK_{i-G}$

四个基本假设如下。

A1. $S \mid\equiv IoTD_i \mid\Rightarrow (\boldsymbol{C_i}, \boldsymbol{e}_i)$

A2. $IoTD_i \mid\equiv S \mid\Rightarrow (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

A3. $G \mid\equiv S \mid\Rightarrow \{\boldsymbol{C_i}, \boldsymbol{M_i}'\}_{TK_{G-S}}$

按照如下步骤，基于假设和BAN逻辑规则，证明了单个ME/IoTD的接入认证协议可以实现上述安全目标。

根据*M1*，可以得到：

Step 1. $S \lhd (\boldsymbol{C_i}, \boldsymbol{e}_i)$

由于$\boldsymbol{C_i}$中随机矩阵$\boldsymbol{S_i}$和$\boldsymbol{X_i}$的存在以及新鲜性规则，可以得到：

Step 2. $S \mid\equiv \sharp(\boldsymbol{C_i}, \boldsymbol{e}_i)$

根据提出的单个ME/IoTD的接入认证协议，目标卫星通过验证签名$\boldsymbol{e_i}$认证每个$IoTD_i$。如果验证成功，可以得到：

Step 3. $S \mid\equiv IoTD_i \mid\sim (\boldsymbol{C_i}, \boldsymbol{e}_i)$

根据临时值检验规则，可以得到：

Step 4. $S \mid\equiv IoTD_i \mid\equiv (\boldsymbol{C_i}, \boldsymbol{e}_i)$

根据*A1*和仲裁规则，可以得到：

Step 5. $S \mid\equiv (\boldsymbol{C_i}, \boldsymbol{e}_i)$，满足*G1*.

根据*M2*，可以得到：

Step 6. $IoTD_i \lhd (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

由于随机矩阵的使用以及新鲜性规则，可以得到：

Step 7. $IoTD_i \mid\equiv \sharp(MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

根据提出的单个ME/IoTD的接入认证协议，每个$IoTD_i$通过检查MAC_S认证目标卫星。如果认证成功，可以得到：

Step 8. $IoTD_i \mid\equiv S \mid\sim (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

根据临时值检验规则，可以得到：

Step 9. $IoTD_i \mid\equiv S \mid\equiv (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

根据信念规则，可以得到：

Step 10. $IoTD_i \mid\equiv S \mid\equiv \boldsymbol{M_i}'$，满足*G2*.

根据*A2*，*Step 9*以及仲裁规则，可以得到：

Step 11. $IoTD_i \mid\equiv (MAC_S, \boldsymbol{U_G}, \boldsymbol{M_S})$

在提出的单个ME/IoTD的接入认证协议中，$IoTD_i$计算会话密钥$TK_{i-G} = H_3(\boldsymbol{S_i}^t \boldsymbol{U_G} \, modq \, mod2)$，其中$\boldsymbol{S_i}$是由$IoTD_i$选取的随机矩阵。另外，根据信念规则，可以得到：

Step 12. $IoTD_i \mid\equiv TK_{i-G}$，满足*G3*.

根据*M3*，可以得到：

Step 13. $G \lhd \{\boldsymbol{C_i}, \boldsymbol{M_i}'\}_{TK_{G-S}}$

由于TK_{G-S}是目标卫星和目标GS在预协商阶段协商完成的，可以得到：

Step 14. $G \mid\equiv S \mid\sim (\boldsymbol{C_i}, \boldsymbol{M_i}')$

由于$\boldsymbol{C_i}$中随机矩阵$\boldsymbol{S_i}$和$\boldsymbol{X_i}$的使用以及新鲜性规则，可以得到：

Step 15. $G \mid\equiv \sharp(\boldsymbol{C_i}, \boldsymbol{M_i}')$

根据临时值校验规则，可以得到：

Step 16. $G \mid\equiv S \mid\equiv (\boldsymbol{C_i}, \boldsymbol{M_i}')$

根据*A3*和仲裁规则，可以得到：

Step 17. $G \mid\equiv (\boldsymbol{C_i}, \boldsymbol{M_i}')$

由于目标GS计算会话密钥$TK_{i-G} = H_3((\boldsymbol{C_i} - \boldsymbol{M_i}')^t \boldsymbol{Y_G} \, modq \, mod2)$，其中$\boldsymbol{Y_G}$是由目标GS选取的，因此，可以得到：

Step 18. $G \mid\equiv TK_{i-G}$，满足*G4*.

通过*Step 5*、*Step 10*、*Step 12*以及*Step 18*可以证明提出的单个ME/IoTD的接入认证协议可以满足相互认证和密钥协商。

5.4.3 非形式化安全分析

本小节采用非形式化安全分析证明了提出的方案可以实现一些重要的安全属性以及抵抗几种已知的协议攻击。

（1）相互认证

卫星与IoT群组之间的相互认证可以成功完成。一方面，目标卫星可以通过如下步骤认证IoT群组。首先，TST通过等式$\| \boldsymbol{e_i} \| \leq \sigma\sqrt{m+1}$验证每个$IoTD_i$生成的基本签名$\boldsymbol{e_i}$，然后用其私钥$\boldsymbol{T_T}$执行半聚合签名机制将所有签名$\boldsymbol{e_i}$转化为一个单一的签名$\boldsymbol{e_0}$, $\boldsymbol{e_g}$和$\boldsymbol{e_{last}} = \{e_{1_{last}}, ..., e_{L_{last}}\}^t$。随后，目标卫星验证$\| \boldsymbol{e_g} \| \leq \sigma\sqrt{m+1}$并且检查等式$\boldsymbol{A_T e_g} \stackrel{?}{=} H_5(\boldsymbol{e_0}||\boldsymbol{e_{last}}) \, mod \, q$和$\boldsymbol{A}_N \, \boldsymbol{e_0} + \boldsymbol{tid_1}' \, e_{1_{last}} + ... + \boldsymbol{tid_L}' \, e_{L_{last}} \stackrel{?}{=} H_1(\boldsymbol{M}_1') + ... + H_1(\boldsymbol{M}_L') \, mod \, q$，该等式等价于验证每个$IoTD_i$签名$\boldsymbol{e_i}$的等式$\boldsymbol{A}_i \, \boldsymbol{e_i} \stackrel{?}{=} H_1(\boldsymbol{M}_i') \, mod \, q$和$\| \boldsymbol{e_i} \| \leq \sigma\sqrt{m+1}$。因此，攻击者产生一个有效的签名等价于解决$ISIS_{q,m,\sigma\sqrt{m+1}}$。另一方面，由于只有指定的卫星可以获得每个$IoTD_i$的隐私信息$\boldsymbol{M_i}$，进而产生有效的$C_S$，因此$IoTD_i$可以通过等式$H_4(H_1(\boldsymbol{M_i} \oplus \boldsymbol{M_S}), \boldsymbol{U_G}) \stackrel{?}{=} C_S \, mod \, z_i$ 成功认证卫星。

（2）条件匿名和不可链路性

由于$IoTD_i$的临时标识取代了真实标识包含在$\boldsymbol{M_i}$中，并且采用了目标卫星的公钥A_S加密后传输。攻击者没有目标卫星的私钥是不可能获得每个$IoTD_i$的临时标识，且只有目标卫星和目标GS才可以获得临时标识。此外，只有NCC可以从临时标识中解析出真实标识，因此提出的方案可以提供条件匿名性。另外，由于随机数z_i和随机矩阵$\boldsymbol{S_i}$ 和$\boldsymbol{X_i}$的使用，攻击者无法判断两条消息是否来自同一个$IoTD_i$，因此，提出的方案可以提供不可链路性。

（3）密钥协商和完美前向、后向安全

每个会话中的会话密钥依赖于参数$(\boldsymbol{C_i}, \boldsymbol{M_i}', \boldsymbol{Y_G})$或$(\boldsymbol{S_i}, \boldsymbol{U_G})$，其中只有$\boldsymbol{C_i}$ 和$\boldsymbol{U_G}$是公开的。由上可知，攻击者不可能获得$\boldsymbol{M_i}'$，且从$\boldsymbol{U_G} \equiv \boldsymbol{A_S}' \, \boldsymbol{Y_G} \, mod \, q$，$\| \boldsymbol{Y_G} \| \leq \beta$中算出$\boldsymbol{Y_G}$，等价于解决$ISIS_{q,m,\beta}$。与此同时，由于在每个密文$\boldsymbol{C_i}$中都存在一个噪声矩阵$\boldsymbol{X_i}$，攻击者无法从$\boldsymbol{C_i}$中计算得到$\boldsymbol{S_i}$。因此，提出的方案可以安全地协商会话密钥。另外，即使$IoTD_i$/目标卫星/目标GS的私钥都丢失，攻击者没有$\boldsymbol{S_i}$/$\boldsymbol{Y_G}$也不可能算出会话密钥，因此，提出的方案可以保证完美前向、后向安全。

（4）抵抗重放、假冒和中间人攻击.

由于在每个会话中都采用了随机数z_i和随机矩阵$(\boldsymbol{X_i}, \boldsymbol{S_i})$，提出的方案可以抵抗

重放攻击。此外，由于IoT群组和目标卫星成功完成了相互认证，因此提出的方案可以抵抗假冒攻击。进而，由于攻击者无法伪造为目标卫星或者$IoTD_i$，因此，提出的方案可以抵抗中间人攻击。

表 5.2　安全对比

方案 / 安全属性	Zhao[38]	Meng[39]	Xue[40]	Yang[41]	我们的方案
相互认证	√	√	√	√	√
条件匿名	√	√	√	√	√
不可链路性	×	×	×	√	√
密钥协商	√	√	√	√	√
完美前向、后向安全	×	×	×	√	√
抵抗协议攻击	√	√	√	√	√
抵抗量子攻击	×	×	×	×	√

最后，表5.2列出了我们提出的方案与其他相关方案满足的安全属性。

5.5　性能分析

本小节，对比了我们方案与其他相关方案在信令开销和传输开销方面的性能。对比方案包括Zhao的方案[38]、Meng的方案[39]、Xue的方案[40] 以及Yang 的方案[41]。不失一般性，假设群成员的数量为L，而对于文献[38–41]中的方案，假设并发激活认证过程的设备数量为L。

5.5.1　信令开销

表 5.3　L个IoTD的信令开销

方案	信令开销
Zhao[38]	$4L$
Meng[39]	$3L$
Xue[40]	$3L$
Yang[41]	$3L$
单个ME/IoTD的接入认证协议	$3L$
海量IoTD的接入认证协议	$L+4$

在信令开销方面，基于L个IoTD的总的信令消息数量评估了我们的方案与其他相关方案。如表5.3所示，Meng的方案[39]、Xue的方案[40]、Yang的方案[41]以及我们提出的单个ME/IoTD的接入认证协议由于没有采用组认证机制耗费了$3L$个信令消

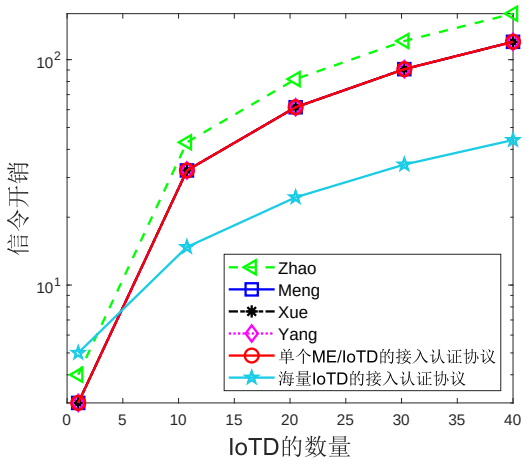


图 5.6 信令开销对比

息。Zhao的方案[38]由于地基节点的额外参与而耗费了$4L$个信令消息。我们提出的海量IoTD的接入认证协议只耗费了$L+4$个信令消息，包括一个卫星认证通知消息，L个用户认证请求消息，一个组认证请求消息，一个组认证响应消息以及一个组认证通知消息。

图5.6展示了我们方案与其他方案随着IoTD并发接入数量增加的信令消息总数量的对比结果。从图5.6可知，由于采用了群组接入认证机制，我们提出的海量IoTD的接入认证协议明显比其他方案耗费更少的信令开销，因此可以有效降低海量IoTD并发接入时的信令冲突风险。其他方案由于并未采用群组接入认证机制，所以耗费较多的信令开销，可能导致信令冲突等问题。

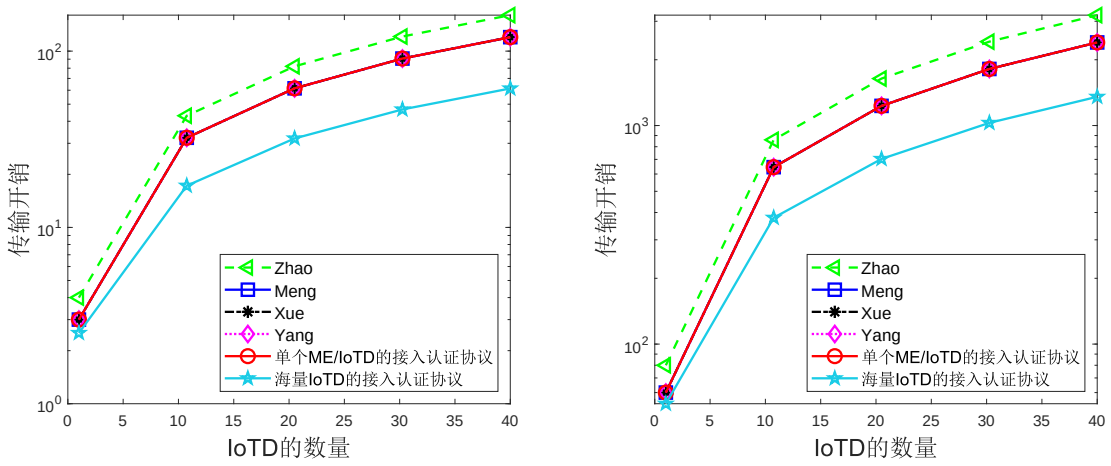
5.5.2 传输开销

表 5.4 L个IoTD的传输开销

方案	传输开销
Zhao[38]	$4Lb$
Meng[39]	$3Lb$
Xue[40]	$3Lb$
Yang[41]	$3Lb$
单个ME/IoTD的接入认证协议	$3Lb$
海量IoTD的接入认证协议	$La+Lb+a+b+c$

针对L个IoTD的传输开销，假设IoTD和TST之间传输一个消息的开销为a，GS/IoTD与卫星之间传输一个消息的开销为b。由于卫星与IoTD/TST/GS距离远大于IoTD与TST之间的距离，因此$a \ll b$。另外，在提出的海量IoTD的接入认证协议中，由于执行了半聚合签名机制，传输开销大幅度减少，假设TST与卫星距离

为c且$c<Lb$。表5.4 中列出了我们方案与其他方案的传输开销。对于Meng的方案[39]、Xue的方案[40]、Yang的方案[41]以及我们提出的单个ME/IoTD的接入认证协议，可以得到其传输开销为$3Lb$。对于Zhao的方案[38]，可以得到其传输开销至少为$4Lb$。我们提出的海量IoTD 的接入认证协议的传输开销为$La+Lb+a+b+c$，具体包括卫星认证通知消息的开销为a，L个用户认证请求消息的开销为La，群组认证请求消息的开销为c，群组认证响应消息的开销为b以及群组认证通知消息的开销为Lb。



(a) $b=1, c=Lb/2$　　(b) $b=20, c=2Lb/3$

图 5.7　传输开销对比

为了简化分析，设置了两组数据：$a=0.01, b=1, c=Lb/2$和$a=0.01, b=20, c=2Lb/3$。图5.7显示了随着并发IoTD数量增加的传输开销的对比结果。从图5.7(a)和图5.7(b) 可知，由于采用了群组接入认证机制，我们提出的海量IoTD的接入认证协议的传输开销明显优于其他方案。

讨论: 综上所述，根据表5.2中的安全对比结果，以及图5.6和图5.7中的性能分析对比结果，我们提出的单个ME/IoTD的接入认证协议和海量IoTD的接入认证协议具有如下优势：

（**1**）我们提出的海量IoTD的接入认证协议和单个ME/IoTD的接入认证协议可以抵抗量子攻击，因此，与Zhao的方案[38]、Meng的方案[39]、Xue的方案[40]以及Yang的方案[41]相比，我们提出的方案更适用于未来的卫星通信网络。与此同时，相比于其他方案，我们提出的方案可以实现更多重要的安全属性包括不可链路性和完美前向、后向安全。

（**2**）与Zhao的方案[38]、Meng的方案[39]、Xue的方案[40]以及Yang的方案[41]相比，我们提出的海量IoTD 的接入认证协议由于采用了群组认证机制而耗费较少的信令和传输开销，因此，我们提出的方案可以有效减低海量IoTD并发接入卫星网络时的信令冲突风险且降低传输负荷。

5.6 结论

本章节基于格理论密码学提出了一个抗量子的终端接入卫星网络的认证方案。该方案主要包括两种类型的认证协议：海量IoTD的接入认证协议和单个ME/IoTD的接入认证协议。我们提出的两个协议可以实现一些重要的安全属性包括相互认证、条件匿名、不可链路性、安全密钥协商、完美前向、后向安全以及抵抗多种协议攻击和量子攻击。安全和性能分析结果表明我们的方案可以提供健壮的安全性且同时可以防止信令冲突、降低传输负荷等。

第六章　工作总结及展望

6.1　工作总结

为满足日益增长的用户通信需求，3GPP网络空口引入了多种不用类型的实体和技术，而新空口实体和技术的引入也带来了一系列的安全和性能问题。本文系统的分析了引入新空口实体和技术所带来的不同的安全和性能问题，并提出了相应的解决办法。

（1）LTE-A网络中为了解决室内覆盖较弱的问题，引入HeNB解决了家庭特色覆盖和业务需求。但是，HeNB的引入导致LTE-A网络切换场景异常复杂等问题，所以设计了一个适应于LTE-A网络中多种类型基站共存的的终端统一切换认证方案。该方案不仅可以应用于LTE-A网络中所有的移动切换场景，而且可以实现健全的安全属性，包括相互认证、密钥协商、隐私保护以及完美前向、后向安全等。此外，安全和性能评估结果表明，该方案不仅能够提供健壮的安全属性，还具有合理的效率。

（2）5G网络支持高速传输，而高速传输最典型的场景就是高铁网络，为了给高铁网络中的用户终端提供平滑的用户通信体验，3GPP引入了车载MRN。但是，MRN的引入导致了新的安全问题例如易遭受窃听攻击、假冒攻击等，以及当前3GPP定义的MRN的切换认证机制仍然无法为用户提供平滑的通信体验且可能导致切换认证失败等问题，所以设计了5G高铁网络中MRN的群组预切换认证方案。该方案包括两种协议：轻量级群组预切换认证协议FTGPHA1和强安全群组预切换认证协议FTGPHA2。在这两个方案中，MRN可以在到达下一个基站的覆盖范围之前与下一个基站提前完成切换认证，从而为用户终端提供较为平滑的通信体验。安全和性能评估结果显示方案FTGPHA1在通信和计算开销方面更加高效，而方案FTGPHA2提供更健壮的安全属性，且耗费合理的切换开销。

（3）为实现全球网络覆盖，3GPP 5G Rel-17中引入了卫星网络接入技术，但是卫星接入技术的引入导致了新的安全问题例如易遭受窃听攻击、假冒攻击等，星地认证时延过长以及海量IoTD并发接入卫星网络导致信令冲突等问题。因此，基于格理论密码学提出了一个抗量子的卫星网络中终端接入认证方案。该方案主要包括两种类型的认证协议：海量IoTD的并发接入认证协议和单个ME/IoTD 的接入认证协议。这两个协议可以实现一些重要的安全属性包括相互认证、条件匿名性、不可链路性、安全密钥协商、完美前向、后向安全以及抵抗多种协议攻击和量子攻击。安全和性能分析结果表明此方案可以提供健壮的安全性且同时可以防止信令冲突、降

低传输负荷等。

6.2 工作展望

论文针对3GPP 网络中引入新空口实体和技术所带来的不同的安全和性能问题进行了初步的探索和研究，并取得了一些研究成果。但是随着研究内容的不断深入，我们发现还有一些研究问题需要进一步深入探索和研究，这也是我们未来努力研究的重点方向，这些问题主要包括：

（1）在5G高铁网络中，MRN的引入增加了终端切换场景的复杂性。例如，列车用户在上下车的过程中，用户终端需在MRN接入点和地面基站接入点之间执行切换认证过程。因此，针对5G高铁网络中的MRN，设计灵活、统一的切换认证机制是未来重点研究方向之一。

（2）本论文中提出的终端接入卫星网络的认证方案中，陆地通信网络中的地面控制中心负责终端的注册、认证和授权等。而在5G网络认证方案中，注册、认证和授权由5G 核心网中特定的组件负责，例如移动性管理实体，归属网络服务器等。因此，该方案并未完全与当前的5G网络认证方案融合。终端接入卫星网络和地面基站网络需要执行不同的接入认证机制，这无疑会增加用户终端以及整个网络的负荷。因此，设计适合于5G卫星网络融合场景下的终端统一接入认证机制是今后亟需解决的问题。

（3）在5G车联网中，车辆可以通过路侧移动单元连接至网络，提供车辆高精度定位、高精度地图等服务。但是路侧移动单元的引入也带来了一些新的挑战。首先，路侧移动单元需要获取手机终端和车辆的路径信息，而这些敏感数据的泄露会增加安全威胁。其次，大量的车辆设备并发接入路侧移动单元可能会导致信令冲突等问题。因此，针对5G车联网场景中的海量车辆联网设备，设计隐私保护的群组认证方案是未来研究工作之一。

参考文献

[1] ELNASHAR A, EL-SAIDNY M A. LTE and LTE-A Overview[M] // Practical Guide to LTE-A, VoLTE and IoT: Paving the way towards 5G. 2018 : 1 – 86.

[2] Global mobile Suppliers Association. GSA Report[EB/OL]. (2020-05). https://gsacom.com/reports/.

[3] 赵玉霞. 5G关键业务场景的专利分析[J]. 信息记录材料, 2019, 20(1) : 239 – 241.

[4] 刘婷宜. 中国电信陈鹏:5G R17标准工作已启动暂定明年9月完成冻结[J]. 通信世界, 2020(19) : 16 – 17.

[5] 马嘉璐. 5G将和4G长期共存2025年5G用户将达8.16亿户[J]. 科学大观园, 2020(2) : 32 – 33.

[6] 张荣涛. 浅析5G与4G网络协同策略研究[J]. 数字技术与应用, 2020, 38(2) : 23,86.

[7] BOEGERGING L. 以4GLTE启程,开始您的5G之旅[J]. 电子产品世界, 2020, 27(5) : 26 – 29.

[8] SESIA S, TOUFIK I, BAKER M. LTE - The UMTS Long Term Evolution[M]. United Kingdom : John Wiley and Sons, 2009 : 437 – 440.

[9] IMT-2020(5G)推进组. 5G愿景与需求[R]. 中国 : IMT-2020, 2014.

[10] KONG Q L, LU R X, CHEN S, et al. Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks[J]. IEEE Internet of Things Journal, 2017, 4(1) : 29 – 39.

[11] PAN M-S, LIN T-M, CHEN W-T. An Enhanced Handover Scheme for Mobile Relays in LTE-A High-Speed Rail Networks[J]. IEEE Transactions on Vehicular Technology, 2015, 64(2) : 743 – 756.

[12] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Feasibility study on LTE relay node security(Release 10) : 3GPP TR 33.816 V10.0.0[R]. 2011.

[13] 3rd Generation Partnership Project. Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA);Study on mobile relay(Release 12) : 3GPP TR 36.836 V12.0.0[R]. 2014.

[14] 3rd Generation Partnership Project. Technical Specification Group Radio Access Network; NR; NR and NG-RAN Overall Description; Stage 2(Release 16) : 3GPP TS 38.300 V16.3.0[R]. 2020.

[15] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system(Release 16) : 3GPP TS 33.501 V16.4.0[R]. 2020.

[16] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Study on using Satellite Access in 5G;Stage 1(Release 16) : 3GPP TR 22.822 V16.0.0[R]. 2018.

[17] JIANG C X, WANG X X, WANG J, et al. Security in space information networks[J]. IEEE Communications Magazine, 2015, 53(8) : 82 – 88.

[18] ZHENG G, ARAPOGLOU P-D, OTTERSTEN B. Physical Layer Security in Multibeam Satellite Systems[J]. IEEE Transactions on Wireless Communications, 2012, 11(2) : 852 – 863.

[19] WU Z F, HU G Y, YOUNES S, et al. A simple real-time handover management in the mobile satellite communication networks[C] // 17th Asia-Pacific Network Operations and Management Symposium. 2015 : 175 – 179.

[20] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 16) : 3GPP TS 23.401 V16.8.0[R]. 2020.

[21] KIM Y, REN W, JO J-Y, et al. SFRIC: A Secure Fast Roaming Scheme in Wireless LAN Using ID-Based Cryptography[C] // IEEE International Conference on Communications. 2007 : 1570 – 1575.

[22] JING Q, ZHANG Y Q, FU A M, et al. A Privacy Preserving Handover Authentication Scheme for EAP-Based Wireless Networks[C] // Global Communications Conference. 2011 : 1 – 6.

[23] CHOI J, JUNG S. A handover authentication using credentials based on chameleon hashing[J]. IEEE Communications Letters, 2010, 14(1) : 54 – 56.

[24] CAO J, LI H, MA M D, et al. A simple and robust handover authentication between HeNB and eNB in LTE networks[J]. Computer Networks, 2012, 56(8) : 2119 – 2131.

[25] QIU Y, MA M D, WANG X L. A proxy signature-based handover authentication scheme for LTE wireless networks[J]. Journal of Network and Computer Applications, 2017, 83 : 63 – 71.

[26] BASIN D, DREIER J, HIRSCHI L, et al. A Formal Analysis of 5G Authentication[C] // ACM SIGSAC Conference on Computer and Communications Security. 2018 : 1383 – 139.

[27] TIAN L, LI J, HUANG Y, et al. Seamless Dual-Link Handover Scheme in Broadband Wireless Communication Systems for High-Speed Rail[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(4) : 708 – 718.

[28] HUANG Q, ZHOU J, TAO C, et al. Mobile Relay Based Fast Handover Scheme in High-Speed Mobile Environment[C] // IEEE Vehicular Technology Conference (VTC Fall). 2012 : 1 – 6.

[29] CAO J, MA M D, LI H, et al. Trajectory prediction-based handover authentication mechanism for mobile relays in LTE-A high-speed rail networks[C] // IEEE International Conference on Communications (ICC). 2017 : 1 – 6.

[30] CAO J, MA M D, LI H. G2RHA:Group-to-Route Handover Authentication Scheme for Mobile Relays in LTE-A High-Speed Rail Networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11) : 9689 – 9701.

[31] HADDAD Z, ALSHARIF A, SHERIF A, et al. Privacy-Preserving Intra-MME Group Handover via MRN in LTE-A Networks for Repeated Trips[C] // IEEE 86th Vehicular Technology Conference (VTC-Fall). 2017 : 1 – 5.

[32] HWANG M-S, YANG C-C, SHIU C-Y. An authentication scheme for mobile satellite communication systems[J]. Operating Systems Review, 2003, 37(4) : 42 – 47.

[33] CHANG Y-F, CHANG C-C. An efficient authentication protocol for mobile satellite communication systems[J]. Operating Systems Review, 2005, 39(1) : 70 – 84.

[34] CHEN T, LEE W-B, CHEN H-B. A self-verification authentication mechanism for mobile satellite communication systems[J]. computers & electrical engineering, 2009, 35(1) : 41 – 48.

[35] CHEN C L, CHENG K W, CHEN Y L, et al. An Improvement on the Self-Verification Authentication Mechanism for A Mobile Satellite Communication System[J]. Applied Mathematics & Information Sciences, 2014, 8(1L) : 97 – 106.

[36] ZHANG C F, WANG X N, LI B L, et al. A novel self-certified security access authentication protocol in the space network[C] // IEEE 14th International Conference on Communication Technology. 2012 : 635 – 639.

[37] ZHENG G, MA H T, CHENG C, et al. Design and logical analysis on the access authentication scheme for satellite mobile communication networks[J]. IET Information Security, 2012, 6(1) : 6 – 13.

[38] ZHAO W W, ZHANG A X, LI J H, et al. Analysis and design of an authentication protocol for space information network[C] // IEEE Military Communications Conference. 2016 : 43 – 48.

[39] MENG W, XUE K P, XU J, et al. Low-Latency Authentication Against Satellite Compromising for Space Information Network[C] // 15th IEEE International Conference on Mobile Ad Hoc and Sensor Systems. 2018 : 237 – 244.

[40] XUE K P, MENG W, LI S H, et al. A Secure and Efficient Access and Handover Authentication Protocol for Internet of Things in Space Information Networks[J]. IEEE Internet of Things Journal, 2019, 6(3) : 5485 – 5499.

[41] YANG Q Y, XUE K P, XU J, et al. AnFRA: Anonymous and Fast Roaming Authentication for Space Information Network[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2) : 486 – 497.

[42] LIU Y C, ZHANG A X, LI J H, et al. An anonymous distributed key management system based on CL-PKC for space information network[C] // IEEE International Conference on Communications, ICC 2016. 2016 : 1 – 7.

[43] CHEN L, JORDAN S, YI-KAI LIU E A. Report on Post-Quantum Cryptography : NISTIR 8105[R]. America : National Institute of Standards and Technology, 2016.

[44] MILLER V S. Use of Elliptic Curves in Cryptography[C] // Advances in Cryptology - CRYPTO. 1985 : 417 – 426.

[45] KOBLITZ N. Elliptic Curve Cryptosystems[J]. Mathematics of Computation, 1987, 48(177) : 203 – 209.

[46] 刘欣东, 徐水帅, 陈建华. 基于椭圆曲线密码的智能电网通信认证协议[J]. 计算机应用, 2019, 39(03) : 779 – 783.

[47] BARKER E. Recommendation for Key Management Part 1-General : NIST Special Publication 800-57 Part 1 (Revision 5)[R]. America : National Institute of Standards and Technology, 2020.

[48] BARKER E, CHEN L, ALLEN ROGINSKY E A. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography : NIST Special Publication 800-56A (Revision 3)[R]. America : National Institute of Standards and Technology, 2018.

[49] CHENG Z H, CHEN L Q. Certificateless Public Key Signature Schemes from Standard Algorithms[J]. IACR Cryptology ePrint Archive, 2018, 2018 : 386.

[50] AL-RIYAMI S S, PATERSON K G. Certificateless Public Key Cryptography[C] // 9th International Conference on the Theory and Application of Cryptology and Information Security. 2003 : 452 – 473.

[51] JI H F, HAN W B, ZHAO L. Certificateless generalized signcryption[J]. IACR Cryptology ePrint Archive, 2010, 2010 : 204.

[52] ZHOU C X, ZHOU W, DONG X W. Provable certificateless generalized signcryption scheme[J]. Designs Codes & Cryptography, 2014, 71(2) : 331 – 346.

[53] TSAI J-L. A New Efficient Certificateless Short Signature Scheme Using Bilinear Pairings[J]. IEEE Systems Journal, 2017, 11(4) : 2395 – 2402.

[54] ISLAM S H, BISWAS G. An Efficient and Provably-secure Digital signature Scheme based on Elliptic Curve Bilinear Pairings[J]. Theoretical and Applied Informatics, 2012, 24(2) : 109 – 118.

[55] HASSOUNA M, BASHIER E, BARRY B I A. A Strongly Secure Certificateless Digital Signature Scheme in the Random Oracle Model[J]. International Journal of Network Security, 2016, 18(5) : 938 – 945.

[56] HUE T T K, HOANG T M, BRAEKEN A. Lightweight signcryption scheme based on discrete Chebyshev maps[C] // 12th International Conference for Internet Technology and Secured Transactions. 2017 : 43 – 47.

[57] ZHENG Y L. Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)[C] // 17th Annual International Cryptology Conference. 1997 : 165 – 179.

[58] KAR J. Provably Secure Identity-based Aggregate Signcryption Scheme in Random Oracles[J].

International Journal of Network Security, 2015, 17(5) : 580 – 587.

[59] ZHOU C X. Identity Based Generalized Proxy Signcryption Scheme[J]. Information Technology And Control, 2016, 45(1) : 13 – 26.

[60] YU H F, YANG B. Pairing-Free and Secure Certificateless Signcryption Scheme[J]. The Computer Journal, 2017, 60(8) : 1187 – 1196.

[61] SHEN X Q, MING Y, FENG J. Identity Based Generalized Signcryption Scheme in the Standard Model[J]. Entropy, 2017, 19(3) : 121.

[62] QI Y F, TANG C M, LOU Y, et al. Certificateless proxy identity-based signcryption scheme without bilinear pairings[J]. China Communications, 2013, 10(11) : 37 – 41.

[63] BONEH D, GENTRY C, LYNN B, et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps[C] // Advances in Cryptology - EUROCRYPT. 2003 : 416 – 432.

[64] SHIM K. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems and Software, 2010, 83(10) : 1873 – 1880.

[65] LAI C Z, LI H, LU R X, et al. SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks[C] // IEEE International Conference on Communications (ICC). 2014 : 1011 – 1016.

[66] CAO J, MA M, LI H. A group-based authentication and key agreement for MTC in LTE networks[C] // Global Communications Conference. 2013 : 1017 – 1022.

[67] 杨明，王兆丽，韩敬利. 基于格的密码学技术专题讲座(一) 第1讲基于格的密码学概述[J]. 军事通信技术, 2014, 35(01) : 67 – 74.

[68] LI F, MUHAYA F B, KHAN M K, et al. Lattice-based signcryption[J]. Concurrency and Computation: Practice and Experience, 2013, 25(14) : 2112 – 2122.

[69] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C] // 40th Annual ACM Symposium on Theory of Computing. 2008 : 197 – 206.

[70] LU X H, YIN W, WEN Q Y, et al. A Lattice-Based Unordered Aggregate Signature Scheme Based on the Intersection Method[J], 2018, 6 : 33986 – 33994.

[71] WANG J Z, WANG C X. Full Secure Identity-Based Encryption Scheme over Lattices in the Standard Model[C] // 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. 2015 : 412 – 415.

[72] GENTRY C, HALEVI S, VAIKUNTANATHAN V. A Simple BGN-Type Cryptosystem from LWE[C] // Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2010 : 506 – 522.

[73] ZHANG P, YU J P, WANG T. A homomorphic aggregate signature scheme based on lattice[J].

Journal of Electronics, 2012, 21 : 701 – 704.

[74] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions (Extended Abstract)[C] // 40th Annual ACM Symposium on Theory of Computing. 2008 : 1 – 7.

[75] 曹春杰. 可证明安全的认证及密钥交换协议设计与分析[D]. 陕西 : 西安电子科技大学, 2008.

[76] 段然, 徐乃阳, 胡爱群. 基于形式化分析工具的认证协议安全性研究[J]. 信息网络安全, 2015(7) : 71 – 76.

[77] 陆思奇, 程庆丰, 赵进华. 安全协议形式化分析工具比较研究[J]. 密码学报, 2014, 1(6) : 568 – 577.

[78] BURROWS M, ABADI M, NEEDHAM R M. A Logic of Authentication[C] // 12th ACM Symposium on Operating System Principles. 1989 : 1 – 13.

[79] 朱宜炳, 罗敏. 典型安全协议形式化分析工具比较[J]. 计算机与现代化, 2008(5) : 86 – 89.

[80] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10) : 1743 – 1756.

[81] 付浩. 安全协议的形式化分析技术方法研究[J]. 电脑知识与技术, 2017, 13(12) : 13 – 14.

[82] 于代荣，杨扬，马炳先等. 基于身份的TLS协议及其BAN逻辑分析[J]. 计算机工程, 2011, 37(01) : 142 – 144+148.

[83] 黄可可，刘亚丽，殷新春. 一种基于PUF的超轻量级RFID标签所有权转移协议[J]. 密码学报, 2020, 7(01) : 115 – 133.

[84] 赵波，向程，张焕国. 一种抵御中间人攻击的可信网络连接协议[J]. 计算机学报, 2019, 42(05) : 1137 – 1148.

[85] 屈娟，冯玉明，李艳平等. 可证明安全的面向无线传感器网络的三因素认证及密钥协商方案[J]. 通信学报, 2018, 39(S2) : 189 – 197.

[86] ODELU V, DAS A K, GOSWAMI A. A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9) : 1953 – 1966.

[87] CAO J, MA M D, FU Y L, et al. CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets[J]. IEEE Transactions on Dependable and Secure Computing, 2019 : 1 – 1.

[88] LI T Y, LIU X D, QIN Z G, et al. Formal Analysis for Security of Otway-Rees Protocol with BAN Logic[C] // International Workshop on Database Technology and Applications. 2009 : 590 – 593.

[89] BLANCHET B, SMYTH B, CHEVAL V, et al. ProVerif Manual[EB/OL]. (2018-05-16). http://prosecco.gforge.inria.fr/personal/bblanche/proverif/manual.pdf.

[90] DOLEV D, YAO A C-C. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2) : 198 – 207.

[91] 郭云川，丁丽，周渊等. 基于ProVerif的电子商务协议分析[J]. 通信学报, 2009, 30(3): 125 – 129.

[92] NEEDHAM R M, SCHROEDER M D. Using Encryption for Authentication in Large Networks of Computers[J]. Commun. ACM, 1978, 21(12): 993 – 999.

[93] WOO T Y C, LAM S S. Authentication for distributed systems[J]. Computer, 1992, 25(1): 39 – 52.

[94] SAXENA N, CHOI B J, LU R X. Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid[J]. IEEE Trans. Information Forensics and Security, 2016, 11(5): 907 – 921.

[95] SUN C, LIU J, XU X P, et al. A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs[J]. IEEE Access, 2017, 5: 24012 – 24022.

[96] CAO J, YAN Z, MA R H, et al. LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks[J]. IEEE Internet of Things Journal, 2020, 7(6): 5329 – 5344.

[97] ZHANG J J, YANG L, CAO W P, et al. Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif[J]. IEEE Access, 2020, 8: 23674 – 23688.

[98] Tamarin Manual[EB/OL]. (2018-11-27). https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf.

[99] YU J S, RYAN M, CREMERS C. DECIM: Detecting Endpoint Compromise In Messaging[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 106 – 118.

[100] BASIN D A, CREMERS C J F, KIM T H, et al. ARPKI: Attack Resilient Public-Key Infrastructure[C] // ACM SIGSAC Conference on Computer Communications Security. 2014: 382 – 393.

[101] BASIN D A, RADOMIROVIC S, SCHMID L. Alethea: A Provably Secure Random Sample Voting Protocol[C] // 31st IEEE Computer Security Foundations Symposium. 2018: 283 – 297.

[102] PALANISWAMY B, CAMTEPE S, FOO E, et al. An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3107 – 3122.

[103] CREMERS C, HORVAT M, SCOTT S, et al. Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication[C] // IEEE Symposium on Security and Privacy (SP). 2016: 470 – 485.

[104] LU B, CAO R H, LU Y M, et al. Design and Formal Analysis of an Authentication Protocol, eWMDP on Wearable Devices[J]. IEEE Access, 2019, 7: 97771 – 97783.

[105] 3rd Generation Partnership Project. Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description;(Release 16): 3GPP TS 36.300 V16.3.0[R].

2020.

[106] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Release 16) : 3GPP TS 22.220 V16.0.0[R]. 2020.

[107] ZHANG A Q, WANG L, YE X R, et al. Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(3) : 662 – 675.

[108] 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE);Security architecture(Release 16) : 3GPP TS 33.401 V16.3.0[R]. 2020.

[109] BLANCHET B. ProVerif[EB/OL]. (2020-05-26). http://prosecco.gforge.inria.fr/personal/bblanche/proverif/.

[110] OPENSSL[EB/OL]. (2020-05-16). http://www.openssl.org/.

[111] OpenPairing[EB/OL]. (2016-02-03). https://github.com/dfaranha/OpenPairing.

[112] FU A M, LAN S H, HUANG B, et al. A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks[J]. IEEE Communications Letters, 2012, 16(11) : 1744 – 1747.

[113] FU A M, ZHAN G X, ZHANG Y Q, et al. GHAP: An Efficient Group-based Handover Authentication Mechanism for IEEE 802.16m Networks[J]. Wireless Personal Communications, 2013, 70(4) : 1793 – 1810.

[114] CAO J, LI H, MA M D. GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks[C] // IEEE International Conference on Communications (ICC). 2015 : 3020 – 3025.

[115] CAO J, LI H, MA M D, et al. UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks[C] // IEEE International Conference on Communications (ICC). 2015 : 7246 – 7251.

[116] NUNES B A A, MENDONCA M, NGUYEN X, et al. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks[J]. IEEE Communications Surveys and Tutorials, 2014, 16(3) : 1617 – 1634.

[117] DUAN X Y, WANG X B. Authentication handover and privacy protection in 5G hetnets using software-defined networking[J]. IEEE Communications Magazine, 2015, 53(4) : 28 – 35.

[118] ARKKO J, LEHTOVIRTA V, ERONEN P. Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') : IETF RFC 5448[R]. 2009.

[119] Tamarin[EB/OL]. (2019-01-18). http://www.infsec.ethz.ch/research/software/tamarin.html.

[120] LU Q L K D M X. Achieving Secure CoMP Joint Transmission Handover in LTE-A Vehicular Networks[C] // IEEE 86th Vehicular Technology Conference (VTC-Fall). 2017 : 1 – 5.

[121] DI B, ZHANG H L, SONG L Y, et al. Ultra-Dense LEO: Integrating Terrestrial-Satellite Networks Into 5G and Beyond for Data Offloading[J]. IEEE Transactions on Wireless Communications, 2019, 18(1) : 47 – 62.

[122] REN Y, OLESHCHUK V, LI F Y. An efficient Chinese remainder theorem based node capture resilience scheme for Mobile WSNs[C] // IEEE International Conference on Information Theory and Information Security. 2010 : 689 – 692.

致谢

光阴似箭，白驹过隙，转眼间我的博士生活也将画上完美的句号。回首走过的岁月，心中倍感充实，当我写完这篇毕业论文的时候，有一种如释重负的感觉，感慨良多。此时此刻，以最为诚挚的感谢，感谢所有在博士期间帮助过我的老师、同学、朋友，还有家人，感谢他们无私的支持和帮助。

首先，感谢我的博士生导师冯登国院士。感谢冯老师在博士期间对我严格的要求、悉心的指导、时刻提醒我刻苦学习，努力钻研业务以及端正科研态度。冯老师渊博的知识、精益求精的科研态度、严谨的科研作风、敏锐的学术眼光、高深的学术造诣，给予我的是一生取之不尽、用之不竭的宝贵财富!

其次，感谢我博士期间的指导老师曹进教授。在这三年多的博士科研工作中，曹老师给了我耐心的指导，使我的科研能力有了显著的提高。在我毕业论文的写作和修改过程中，曹老师悉心指导，从论文的选题、论文的具体执行到定稿，都凝结了曹老师的心血和智慧结晶。

感谢在攻读博士学位期间所有授课的老师们!

感谢各位同门师兄弟姐妹，这些年我们一起在埋头苦读、互相鼓励、共同面对困难，这段难忘的人生际遇将成为我永远的美好回忆。

最为感谢我的丈夫何诗洋以及我亲爱的父母，谢谢你们一直以来对我的包容、支持和理解。是他们无私的奉献，才使我能够顺利考入高等学府继续深造。感谢他们对我博士期间无私的支持和帮助，使我能安心完成学业。

谨借此机会向所有给予我关心和帮助的朋友、老师和家人们表示由衷的感谢!

作者简介

1. 基本情况

马如慧，女，陕西榆林人， 1991 年 5 月出生，西安电子科技大学，网络与信息安全学院，网络空间安全专业，2017级博士研究生。

2. 教育背景

2009.08～ 2013.07，西安电子科技大学，学士，专业：信息工程
2013.08～ 2016.01，西安电子科技大学，硕士，专业：电子与通信工程
2017.08～ ，西安电子科技大学，博士，专业：网络空间安全

3. 攻读硕士学位期间的研究成果

3.1 发表学术论文

[1] **Ruhui Ma**, Jin Cao, Dengguo Feng, Hui Li, LAA: Lattice-based Access Authentication Scheme for IoT in Space Information Networks[J], IEEE Internet of Things Journal (IoT), 2020, 7(4):2791-2805. (SCI, EI, 中科院分区1区)

[2] **Ruhui Ma**, Jin Cao, Dengguo Feng, Hui Li, Shiyang He, FTGPHA: Fixed-Trajectory Group Pre-Handover Authentication Mechanism for Mobile Relays in 5G High-Speed Rail Networks[J], IEEE Transactions on Vehicle Technology (TVT), 2020, 69(2):2126-2140(SCI, EI, 中科院分区2区).

[3] **Ruhui Ma**, Jin Cao, Dengguo Feng, Hui Li, Yinghui Zhang, Xixiang Lv, PPSHA: Privacy Preserving Secure Handover Authentication Scheme for All Application Scenarios in LTE-A networks[J], Ad Hoc Networks, 2019, 87:49-60. (SCI, EI, 中科院分区2区)

[4] **Ruhui Ma**, Jin Cao, Dengguo Feng, Hui Li, Ben Niu, Fenghua Li, Lihua Yin, A Secure Authentication Scheme for Remote Diagnosis and Maintenance in Internet of Vehicles[C], IEEE Wireless Communications and Networking Conference (WCNC), 2020, pp. 1-7.(EI, CCF C类)

[5] Jin Cao, Zheng Yan, **Ruhui Ma**, Yinghui Zhang, Yulong Fu, Hui Li, LSAA: A Lightweight and Secure Access Authentication Scheme for both UEs and mMTC Devices in 5G Networks[J], IEEE Internet of Things Journal (IoT), 2020, 7(6):5329-

5344.(第三作者, SCI, EI, 中科院分区1区)

[6] Jin Cao, Maode Ma, Hui Li, **Ruhui Ma**, Yunqing Sun, Pu Yu, Lihui Xiong, A Survey on Security Aspects for 3GPP 5G Networks[J], IEEE Communications Surveys & Tutorials, 2020, 22(1): 170-195. (第四作者, SCI, EI, 中科院分区1区)

[7] **Ruhui Ma**, Jin Cao, Dengguo Feng, Hui Li Yang Xu, A Robust Authentication Scheme for Remote Diagnosis and Maintenance in 5G V2N[J], IEEE Transactions on vehicle technology (TVT)(在投).

[8] **马如慧**, 曹进, 李晖. 高效的隐私保护在线开票服务认证方案[J].通信学报(在投).

3.2 申请（授权）专利

[1] 曹进, **马如慧**, 李晖, 何诗洋. 基于固定路径的群预切换认证方法、高铁网络通信平台, 申请号: 2019100780754, 申请公布号: CN109769248A, 申请公布日:2019.05.17.

[2] 曹进, **马如慧**,卜绪萌, 李晖. 适用于5G网络设备的轻量级安全接入认证方法及应用,申请号: 2019108859586, 申请公布号: CN110768954A, 申请公布日: 2020.02.07.

[3] 曹进, **马如慧**, 陈李兰, 李晖. 卫星网络断续连通场景下的接入和切换认证方法及系统, 申请号: 202010776718.5, 申请日: 2020.08.05.

[4] 曹进, **马如慧**, 李晖, 陈李兰. 适用于天地一体化的群组接入认证和切换认证方法及应用, 申请号: 202010968822. 4, 申请日: 2020.09.15.

[5] 曹进, **马如慧**, 李晖, 关键. 一种多类型终端接入与切换认证方法、系统、设备及应用, 申请号: 202010970241. 4, 申请日: 2020.09.15.

3.3 参与科研项目及获奖

[1] 西安电子科技大学网络与信息安全学院2019年研究生创新基金项目, 5G-V2X场景下的车载移动设备群组接入认证机制研究, 2019.05-2020.05, **项目负责人**, 负责项目整体设计与研究，针对5G网络中高速移动车辆和普通车辆的车载移动设备分别设计了不同的群组认证机制.

[2] 国家自然科学基金面上项目, 未来5G新应用场景下海量多类型终端认证机制研究(61772404), 2018.01-2021.12, **主要参与人**, 负责5G 网络中海量终端高效匿名并发接入认证和密钥协商协议的设计.

[3] 陕西省重点产业创新链（群）-工业领域项目, 云雾混构环境下移动互联网大规模身份管理与认证关键技术研究, 2020.01-2022.12, **主要参与人**, 负责轻

量化基于群组的安全接入认证机制的研究.

[4] 陕西省自然科学基础研究计划面上基金项目, 未来5G场景下的身份认证技术研究(2017JM6029), 2017.01-2018.12, **主要参与人**, 负责海量终端高并发接入认证机制的设计.

[5] OPPO横向课题, 基于5G网络架构的安全增强研究, 2019.10 2020.9, **主要参与人**, 负责深入学习5G-AKA并改进5G-AKA以完成安全接入协议的设计.