基于IMS体制的加密通信关键技术及解决方案研究

Research on Key Technologies and Solutions of Encrypted Communication Based on IMS System

李佳如，刘牧寅，王　亮（中讯邮电咨询设计院有限公司，北京 100048）
Li Jiaru，Liu Muyin，Wang Liang（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
基于网信安全背景，研究IMS体制的加密通信技术架构及解决方案。提出加密通信整体技术架构，并介绍了架构的主要功能模块；同时与核心业务场景结合，设计身份鉴权、一对一加密消息、一对一加密通话等功能与业务流程，探讨了加密通信应用的实际场景和业务价值。最后，对加密通信后续发展进行展望。

关键词：
加密消息；加密通话；加密通信；IMS；数据安全
doi：10.12045/j.issn.1007-3043.2022.09.010
文章编号：1007-3043（2022）09-0044-05
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Based on the background of network information security，it studies the architecture and solution of encrypted communication technology under IMS. The overall technical architecture of encrypted communication is proposed，and the main module functions of the architecture are introduced. In addition，combined with the core business scenario，the functional architecture and business process of identity authentication，1to1 encrypted message and 1to1 encrypted call are designed，and the actual scenario and business value of encrypted communication application are discussed. Finally，the future development of encrypted communication is prospected.

Keywords：
Encrypted message；Encrypted call；Encrypted communication；IMS；Data security

引用格式：李佳如，刘牧寅，王亮. 基于IMS体制的加密通信关键技术及解决方案研究[J]. 邮电设计技术，2022（9）：44-48.

0 引言

随着高带宽、低时延的5G技术飞速发展，移动通信的便捷性、多媒体内容的多样性、交互体验的真实性显著提升。以微信、钉钉、飞书为代表的互联网音视频通信软件为用户提供了极为丰富的沟通手段，几乎替代了运营商传统语音、消息以及其他多媒体沟通方式，逐渐成为个人移动办公、远程会商、生活社交必不可少的载体。然而，随着计算机协议的结构性缺陷逐渐暴露，互联网厂商提供的开放即时通信模式经常发生通话窃听、信息窃取、数据篡改等安全事件[1-2]。一旦泄密将危害国家安全、社会秩序，造成不可估量的损失。

运营商作为国家数字信息基础设施服务的建设者和运营者，致力于向广大用户提供稳定、高质量的基础通信服务。在网络泄密事件频发的背景下，需发挥自身优势，承担央企责任与担当，持续深耕网络加密技术架构及方案研究，增强基础通信安全保障，为国家、社会、个人提供安全保密、协同高效的通信服务能力[3-4]。

IMS网络是电信运营商普遍应用的音视频及多媒体消息业务解决方案，为用户提供语音、视频、图片等

收稿日期：2022-07-14

类型的实时、非实时端到端通信服务。因此，本文结合现有IMS网络架构及加密通信技术现状，提出集安全通信SDK、加密模块、密网服务、业务处理一体化的IMS加密通信技术架构。

1 加密通信现状及传统解决方案

1.1 移动通信现存安全问题

移动通信网络中，用户通信请求依次经过终端、基站、中继及交换设备等传输，并在中心侧或云上的服务设备间进行应用层的路由、存储、转发，由于每个传输环节安全性都需要保证，故终端及网络面临众多潜在安全风险。隐藏于暗处的非法攻击者，利用网络协议和通信系统的弱点进行攻击，给用户和通信网络带来严重损失。通信中的安全威胁主要包括以下4种[5]。

a）窃听：在无线链路或者核心网内进行窃听，获取通信中的用户、信令、控制等数据。

b）伪装：伪装为网络单元或终端来窃取用户、信令、控制等数据，欺骗网络获取服务。

c）数据破坏：修改、重放、插入、删除用户或信令数据，破坏数据完整性。

d）非授权访问：终端或网络滥用权限访问非授权服务和数据。

1.2 传统加密通信技术解决方案

现代移动通信中，核心安全问题是解决数据保密传输。因此传统加密方式常分为以下3种。

a）链路加密：传输数据仅在数据链路层加密，保护通信节点间数据；接收方是传送路径上各节点机，数据到达目的地前，依次在每台节点机解密、加密，此方式无法避免数据传输时节点机产生的明文信息。基于IPSec隧道的VPN技术为链路加密的实例[6]。

b）节点加密：节点处采用与节点机相连的加密装置，密文在其中解密、加密，避免链路中加密节点的明文信息遭受攻击；但此方式需大量加密装置，成本高。常用于电脑网络系统集群结构加密，如CDN系统[7]。

c）端到端加密：为终端间数据加密。除报头外，报文以密文形式贯穿整个传输，仅发送端和接收端可加、解密，减少密码设备数量，避免数据泄露，但需收发方使用同一密钥通信，技术要求较高[8]。

由于端到端加密对数据本身进行加密，保证了数据传输的可靠性，实现和维护空间更大。结合语音通信技术体制，端到端加密衍生了VoIP加密、VoLTE加密等实现手段。

VoIP加密网络架构传输数据采用动态分组加密方法，不同分组采用不同加密算法和密钥加密，保证了数据较安全传输。但VoIP信令一般为私有协议，或基于RFC3261 SIP协议更改，协议层未考虑安全设计，在不同运营商、设备厂商间互通性较差[9]。

VoLTE加密可与AKA算法结合实现用户和网络的双向认证，采用“一请求一密钥”的方式合理有效地协商分配密钥[10]。然而，此方式对运营商网络有强依赖，无法跨境通信，且VoLTE加密通话只支持VoLTE语音模式，对于CSFB、TD-SCDMA/GSM语音模式的单待终端，无法收发加密电话。此外，任何服务网络都能请求网络身份认证，致使服务器无法判断收到的认证是否来自实际用户，给攻击者提供机会。

2 基于IMS体制的加密通信技术架构

2.1 IMS网络架构

IMS架构支持灵活接入，支持移动用户媒体数据传递与管理，满足通信网络对安全、计费、漫游及QoS的需求。此外，延时低、响应迅速、扩展性强等特性也为运营商多媒体通信、加密通信架构提供了良好业务环境及定制化空间[11]。

2.2 整体技术架构

基于IMS架构及加密通信需求，提出的技术架构如图1所示。加密通信网络结构分为用户设备层、网

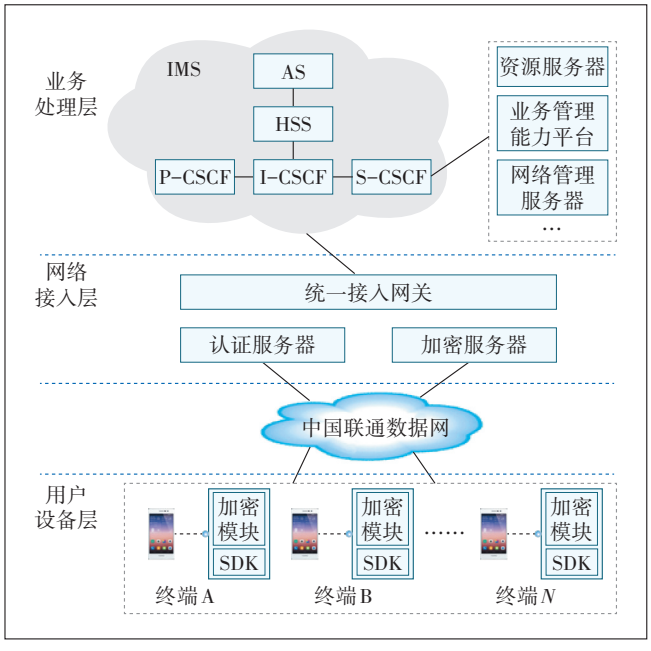

图1　加密通信整体网络架构

络接入层和业务处理层。

a）用户设备层为嵌入加密模块、安全通信SDK的IMS安全终端；通信时，通过网络接入层的密网服务与业务处理层互通。IMS终端为嵌入安全模块的定制终端。接入类型上，分为手机、平板等移动终端，以及IP话机等固定终端；形态上，可分为原生终端或IMS APP客户端。安全通信SDK通过前端界面，展示、处理用户收发的信息，将明文消息传递到内置加密模块进行加密，实现明文信令、流媒体通信加密。

b）网络接入层为此架构的核心定制化部分，由认证服务器、加密服务器、统一接入网关组成，处理来自用户设备层的加密请求，管理证书、密钥、日志及系统信息，执行身份鉴权、呼叫控制。具体功能为：

（a）认证服务器：认证、管理不同终端身份，实现授权、鉴权等功能。

（b）加密服务器：分发、管理加密证书和通信密钥，结合业务场景加解密用户数据。

（c）统一接入网关：检测接入终端及传递信息的合法性，转发合法信息，拦截非法信息。灵活实现系统层对接，降低安全风险。

c）业务处理层为网络架构的业务处理中心。由IMS网络、资源服务器、业务管理能力平台、网络管理服务器构成，对网络接入层转发的请求，进行登录鉴权、加密消息、加密通话、资源分配、网络互通，支持业务场景定制化。

（a）IMS网络：包含P-CSCF、I-CSCF、S-CSCF、HSS及AS等网元；其中P-CSCF与用户设备层相连，负责接收、转发消息，实现资源授权及QoS管理。I-CSCF分配用户服务节点，实现跨运营商域间拓扑隐藏。S-CSCF控制用户的注册鉴权和会话，记录呼叫状态。HSS负责存储用户基本标识、路由信息、业务签约信息。AS为网络架构提供基础增值服务[12]。

（b）资源服务器：控制和处理媒体数据及资源，解析处理多媒体放音、码变换、语音识别[13]。

（c）网络管理服务器：合理管理网络请求，实现负载均衡。

（d）业务管理能力平台：进行第三方业务管理、数据安全管理，实现数据流转、统计查询等功能。

所提出技术架构的业务交互流程为：用户设备层的IMS终端通过内置安全通信SDK发送明文通信请求，该请求经加密模块加密，被传递到中国联通数据网进行处理后再被传递到网络接入层。认证服务器随后鉴别用户身份，通过鉴别的用户会向加密服务器申请证书、密钥；并经过统一接入网关将请求传递到业务处理层，IMS网络会话控制模块寻找到接收端后，将请求传递到接收端，接收端通过加密模块解密，最后安全通信SDK展示解密后的明文信息。该架构利用IMS现网的业务扩展性，与加密服务紧密结合，提升了媒体通信的安全和数据完整性。

3 基于IMS体制的加密通信业务流程

3.1 身份鉴权

为保证数据安全、完整传输，需构建适配终端的用户身份鉴权和私密保护机制。本文设计的身份鉴权，可通过账号与token对应关系及“双鉴权”形式，保护用户信息不被泄露。详细流程见图2。

初始鉴权：终端登录安全通信SDK后，SDK携带开户账号将认证请求传递到加密模块加密，随后加密模块传送该请求到认证服务器，执行初始鉴权，对应步骤①~②。

获取账号token：终端发起鉴权后，认证服务器执行步骤③~④，判断用户的合法性，若合法，返回账号信息及身份token给该终端，若非法，禁止该用户登录。

二次鉴权：对于合法用户，终端携带账号、token，执行步骤⑤~⑩的账号登录，SDK依次通过加密模块、认证服务器，将信息传递到统一接入网关进行身份校验，通过校验的请求会在IMS-HSS模块进行二次鉴权，若信息合法且账号及token存在绑定关系，允许该终端登录；若信息不存在或无绑定关系，禁止该终端登录。

3.2 一对一消息

加密消息收发为安全通信主要场景，收发端传递的消息包含文本、音频、图片、视频、文件等，流程如图3所示。

消息加密：发送方向接收方传递的明文消息通过安全通信SDK传递到加密模块加密，并向加密服务器获取证书、密钥。加密服务器生成证书、密钥，对数据包加密完成后返回给终端，对应步骤①~④；步骤⑤执行接入校验，通过IMS网络寻找接收方。

消息解密：IMS网络收到请求后，执行步骤⑥~⑦寻找接收方。若接收方在线，收到IMS通知后，向加密服务器获取证书、密钥，并通过加密模块将消息解密，通过安全通信SDK获取消息详情，如步骤⑧~⑪；若不在线，再次登录时，将主动拉取消息并进行解密，实现

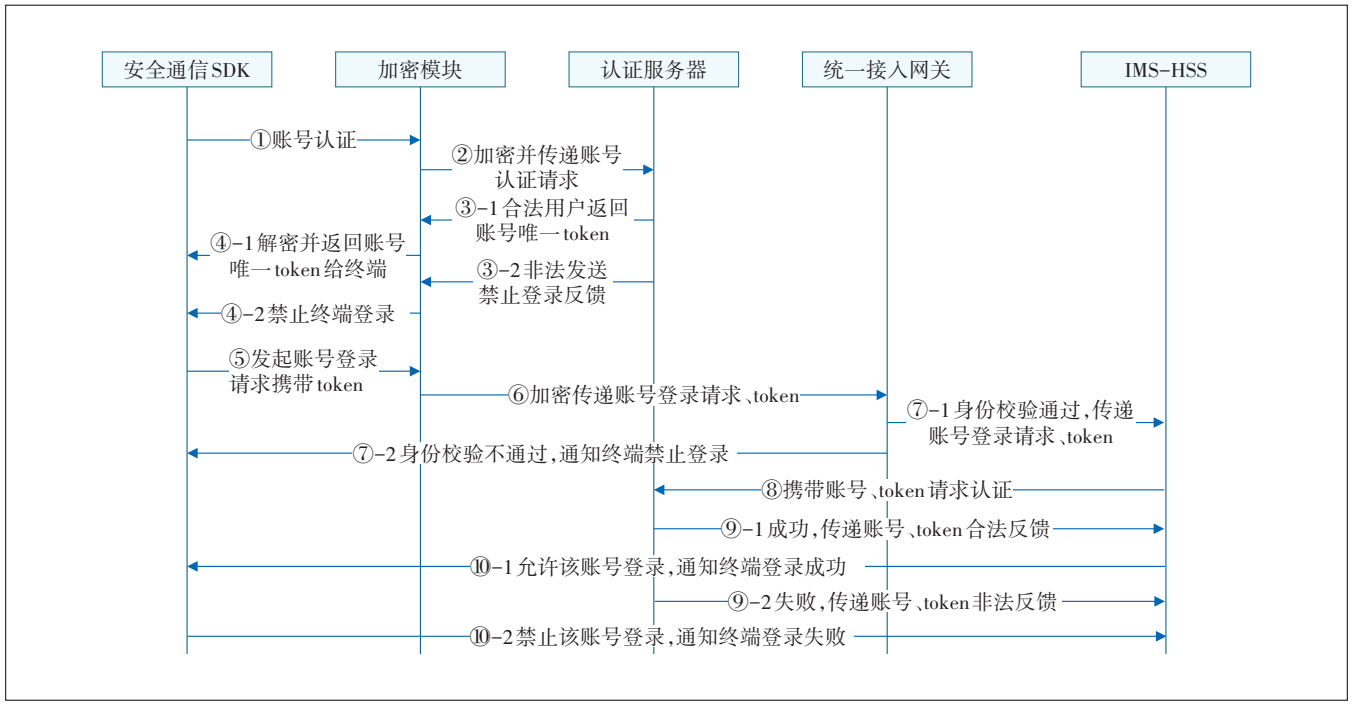

图2　加密通信鉴权

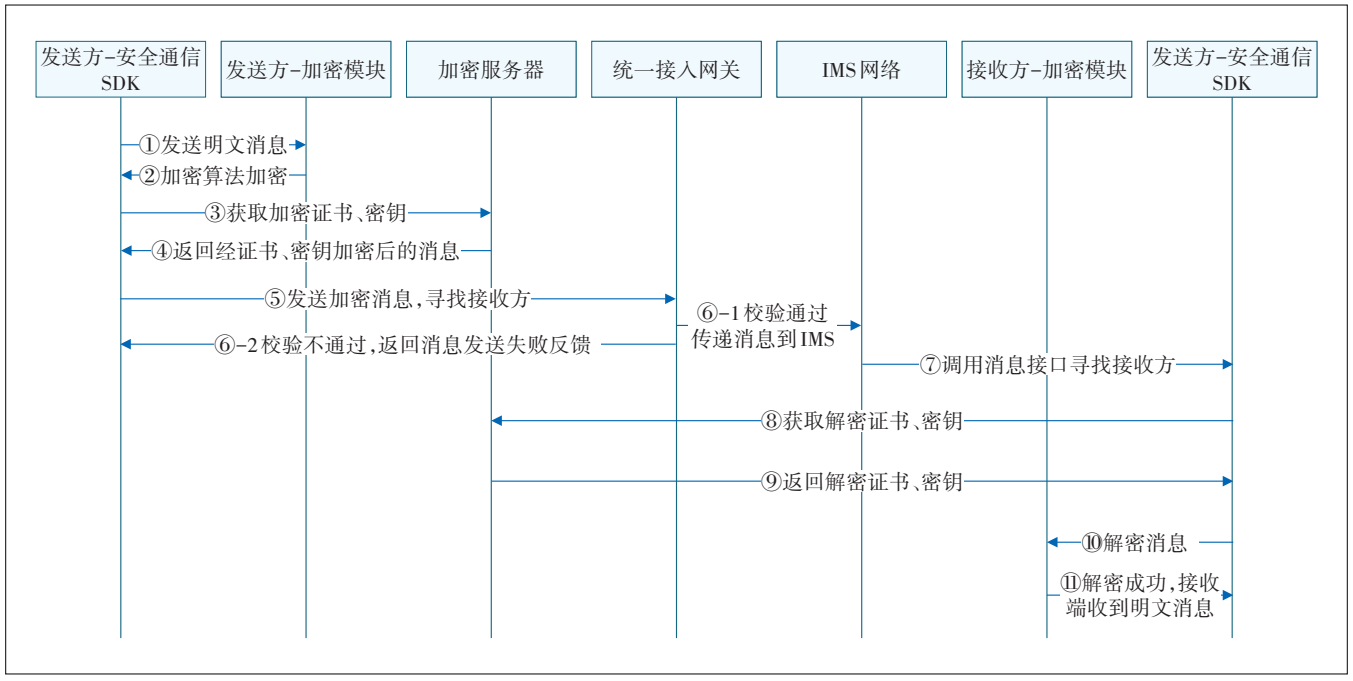

图3　加密通信一对一消息

一对一加密消息收发。

3.3　一对一通话

加密通话保证了信息即时传递和业务交流，故加密通信的另一主要场景为一对一加密通话，详细流程见图4。

一对一加密通话中，主被叫先后建立信令层和媒体层通话请求。

建立信令层请求：主叫用户通过安全通信SDK向被叫发起信令、媒体层的呼叫请求，与加密消息类似，请求经过加密模块传递、加密服务器分配密钥、统一

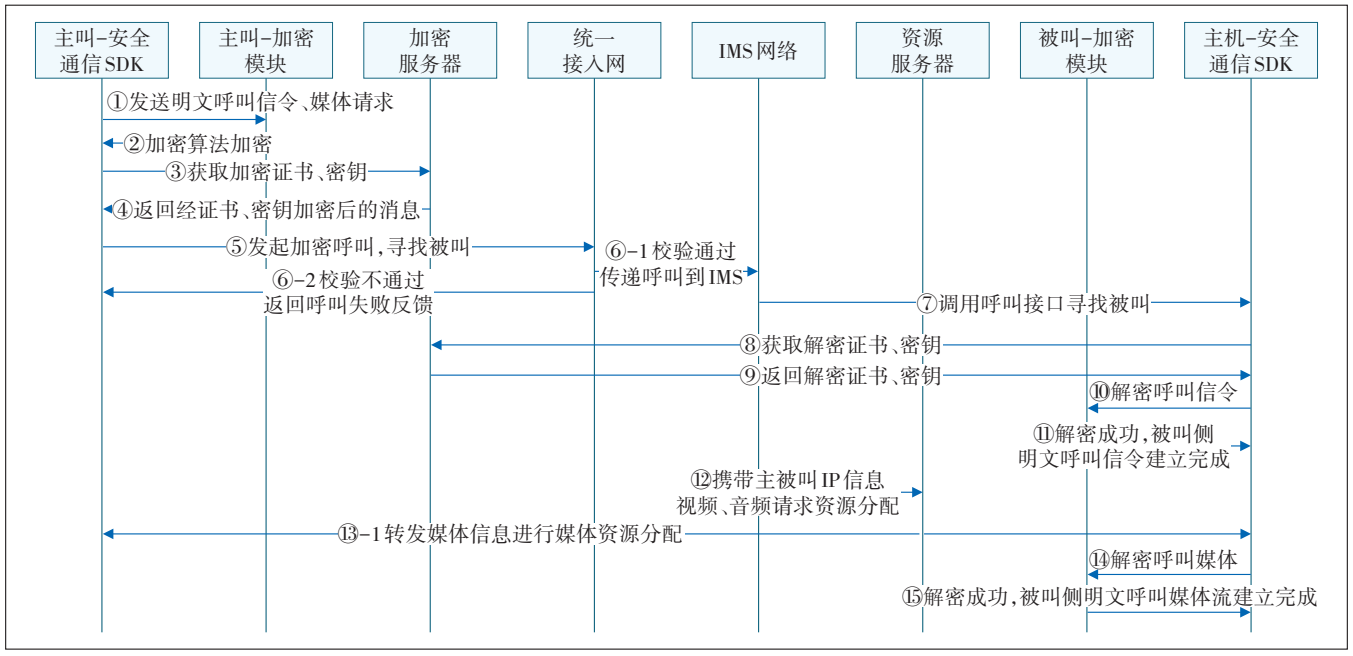

图4　加密通信一对一通话

接入网关校验合法性后，通过IMS网络转发呼叫请求，见步骤①~⑦；被叫接收到请求后，分别经过加密服务器、本端加密模块解密，在安全通信SDK展示主叫通话请求，如步骤⑧~⑪。

信令层请求完成后，建立媒体层请求：如步骤⑫~⑬，IMS网络携带主被叫的IP及音视频信息向资源分配服务器请求资源分配，服务器收到请求分配主被叫资源；主被叫接收通知后，通过自身加密模块解密媒体流，并使用安全通信SDK显示通话，见步骤⑭~⑮。至此，完成加密一对一通话呼叫应答。

4 总结

本文结合移动通信业务安全需求，提出了IMS体制的加密通信技术架构，围绕应用场景，设计身份鉴权、一对一消息、一对一通话的业务流程，以安全终端、安全通信SDK、密网结合的方式为互联网安全通信提供新思路。随着用户安全通信需求提高及5G技术的发展，融合5G音视频与消息技术的加密高清音视频通话、加密富媒体消息等安全多样的解决方案也会逐步推向市场，满足政府机构、企业个人的安全移动办公需求，打造网信安全基础通信业务新生态。

参考文献：

[1] 杨晓雾. 计算机通信网络安全与防护策略[J]. 电信工程技术与标准化，2019(7)：214-218.
[2] 李昱萌. 计算机通信网络安全与防护策略的相关思考[J]. 电子测试，2018(18)：135-136.
[3] 贾晓旭. 互联网通信技术发展下通信运营商创新策略研究[J]. 环球市场，2020(10)：360.
[4] 冯昌杰，王晗，陈厚成. 互联网通信技术发展下通信运营商创新策略研究[J]. 数字通信世界，2019(5)：237-238.
[5] 包鹤，陈天，赵太飞. 第4代移动通信系统安全缺陷分析[J]. 通讯世界，2016(11)：21-22.
[6] 彭凯. 计算机网络通信安全中数据加密技术的应用研究[J]. 计算机与网络，2018(11)：56-57.
[7] 徐晓玲. CDN网络安全风险分析及应对策略研究[J]. 信息网络安全，2020(11)：74-77.
[8] 卢光辉. 试论移动通信端到端加密安全方案设计[J]. 中国新通信，2017(9)：53-53.
[9] 魏占祯，穆文博，曹浩. 基于SIP协议VoIP系统安全问题的研究与分析[J]. 北京电子科技学院学报，2017(25)：36-42.
[10] 陈格. 一种基于安全芯片的VoLTE加密通话方案设计[J]. 广东通信技术，2016(7)：12-15.
[11] 刘春蕾. IMS在通信领域的应用与前景分析[J]. 数字化用户，2018(28)：23，230.
[12] 李秀全. IMS应用及存在的问题探讨[J]. 数字化用户，2019(43)：8.
[13] 罗有平，周炳然. 一种IMS框架下的CSCF实现模型[J]. 军民两用技术与产品，2017(24)：58-59.

作者简介：
李佳如，工程师，硕士，主要从事加密通信技术研究、IMS网络设计、安全终端解决方案等工作；刘牧寅，高级工程师，硕士，主要从事IMS网络、音视频、消息类产品研发工作；王亮，高级工程师，硕士，主要从事终端与业务相关的技术和市场工作。