基于运营商网络的量子加密通信关键技术及方案研究

Research on Key Technologies and Solutions for Quantum Encrypted Communication Based on Operator Networks

李佳如[1]，梁　艳[2]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）
Li Jiaru[1]，Liang Yan[2]（1. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China；2. China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：
结合网信安全背景，研究运营商网络的量子加密通信技术架构及解决方案。利用量子力学特性，生成不可复制、不可预测的量子密钥加解密通信数据，并提出基于量子密钥分发技术的端到端量子加密通信整体技术架构。此外，结合运营商语音业务场景，设计身份认证、一对一加密通话、通信安全监管等功能与业务流程，实现基于量子密钥的加密通信数据安全保障。最后，对量子加密通信的业务价值及后续使用场景进行展望。

关键词：
量子密钥；加密通信；VoLTE；QKD；数据安全
doi：10.12045/j.issn.1007-3043.2026.03.016
文章编号：1007-3043（2026）03-0087-06
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In the context of cybersecurity，it delves into the quantum encryption communication technology architecture and solutions for telecom operator networks. By leveraging the unique properties of quantum mechanics，quantum keys are generated，which are inherently impossible to replicate or predict，and these keys are employed to encrypt and decrypt communication data. An overall technical architecture for end-to-end quantum encryption communication based on Quantum Key Distribution（QKD）technology is proposed. In addition，by integrating with the voice service scenarios of operators，it designs functions and business processes such as identity authentication，one-to-one encrypted calls，and communication security supervision，achieving data security assurance for encrypted communication based on quantum keys. Finally，a perspective is presented on the business value of quantum encryption communication and the subsequent usage scenarios where quantum encryption communication can be applied.

Keywords：
Quantum key；Encrypted communication；VoLTE；QKD；Data security

引用格式：李佳如，梁艳. 基于运营商网络的量子加密通信关键技术及方案研究[J]. 邮电设计技术，2026（3）：87-92.

0 引言

随着移动通信产业的快速发展和移动终端用户数量的不断增长，通信网络的安全问题逐渐显现并引发广泛关注。近年来，伪基站等非法手段的兴起，使得无线截听行为日益猖獗，个人隐私、企业商业秘密甚至国家机密均有可能被外泄。在国家“十四五”规划和2035年远景目标纲要中，“安全”和“网络”被列为重要关键词，网络数据安全已成为建设数字中国的重要基石[1-2]。

在语音业务方面，国内移动通信系统尚未普及端到端的安全防护机制，非法截取信息的风险长期存在，尤其在军事、政府和金融等高敏感领域，对移动通信安全服务的需求尤为迫切。在此背景下，基于量子力学特性的量子密钥分发技术，使通信双方能够产生并分享一个真随机、安全的量子密钥来加/解密信息，

收稿日期：2026-02-09

抵御潜在的网络安全威胁和风险，为端到端通信安全提供了全新路径，也为保护个人隐私和国家信息安全提供了强有力的技术保障[3-4]。

当前，我国运营商网络有2种语音通话方式，即VoNR和VoLTE。本方案基于运营商语音通话网络及量子密钥，针对语音通信，提出端到端量子加密业务解决方案，提出集加密通话SDK、量子密码服务、加密通信业务管理服务、安全监管服务一体化的量子加密通信技术架构，为下一代运营商通信提供了安全性高、兼容性强、可扩展的安全保障产品。

1 加密通信现状及传统解决方案

1.1 移动通信现存的安全问题

工信部2025年公布的数据显示，我国移动通信用户总数已超过47亿，其中4G、5G用户数超过18亿[5]。庞大的用户基数意味着海量的用户手机号码、位置信息、通信内容等关键通信信息被存储在移动通信网络中，如何保障这些数据的安全成为移动通信网络安全机制设计的核心[6-7]。尽管4G、5G网络等移动通信技术不断升级演进，但电信诈骗、企业个人隐私泄密等安全事件频发，通信网络的安全性仍然面临严峻考验。移动通信网络中常见的威胁主要有以下5种[8-9]。

a）信息窃听。攻击者通过截获网络传输中的通信内容，获取用户的敏感信息，如通话内容、短信和数据流量，严重威胁用户隐私。

b）伪装攻击。不法分子伪装为合法用户或网络节点，通过欺骗方式获取访问权限，窃取敏感数据或实施其他恶意操作。

c）数据篡改。通过插入、修改或删除传输中的数据，破坏通信完整性，可能导致信息误传或服务中断。

d）未授权访问。非法终端或用户未经授权访问通信网络，利用系统漏洞获取不属于其权限范围的服务或数据。

e）非接触式攻击。利用移动网络的协议或硬件漏洞实施远程攻击，如窃取用户的地理位置、手机号码或其他敏感信息。

1.2 传统移动通信安全技术及解决方案

面临生活中的各类网信安全问题，移动通信的核心安全挑战在于保障数据传输的机密性和完整性。传统安全通信解决方案主要分为以下4类[10-11]。

1.2.1 身份验证

身份验证是移动通信安全的基础手段之一，该方案通过对通信双方的合法性进行验证，保障通信的安全性和可靠性。传统的身份验证技术包括用户名和密码、双因素认证、基于SIM卡的认证以及PKI证书等。这些技术在实际应用中有效阻止了非法用户的接入，降低了网络被攻击的风险，为通信网络的安全运行提供了有力支持。

1.2.2 密钥加密

密钥加密是保护通信内容免遭窃取和篡改的核心方法，该方法通过将明文数据转化为密文，从而实现数据的保密性。密钥加密主要分为对称加密和非对称加密2种加密方式，对称加密高效，适用于实时通信，而非对称加密密钥管理便利，主要应用于密钥交换与数字签名。

1.2.3 网络安全协议

网络安全协议通过对通信链路的加密和认证，提供可靠的传输保障。常见协议包括IPSec、TLS/SSL和SRTP等，这些协议分别在网络层和传输层对数据进行加密保护，确保通信内容的保密性和完整性。特别是在VoIP和IMS通信中，这些协议的综合使用有效增强了移动通信网络的安全性。

1.2.4 访问控制与威胁防护

访问控制通过限定用户和设备对通信资源的访问权限，减少了未授权访问的风险，常见方式包括基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）。同时，配合入侵检测系统、防火墙和恶意软件检测等威胁防护技术，使通信网络能够实时识别和应对异常行为，为信息安全提供全面保障。

网络安全协议、访问控制与威胁防护在移动通信安全技术中较为常见，但由于2种方式的加密和认证过程会引入额外的通信时延、产生动态流量分析，从而导致响应时间较长，产生较高的计算开销，难以满足实时通信安全场景下对低延迟和高性能的要求。因此，实时通信通常选取身份验证和加密技术，并提供端到端的认证及加密技术，该方案被广泛应用于运营商语音、视频及消息传输中。

2 基于IMS网络架构的量子加密通话

VoLTE和VoNR是现代运营商移动通信网络中用于提供高质量语音服务的关键技术。IMS作为VoLTE和VoNR的核心架构，负责处理语音和多媒体服务的信令控制、会话管理及媒体传输，使VoLTE和VoNR能

够在各自的网络环境下实现高质量的语音通信和多媒体服务。此外，IMS网络架构灵活，其低延迟、扩展性强等特性也为运营商安全通信架构及多媒体解决方案提供了良好业务环境及定制化空间[12-13]。

量子加密通信是融合量子密钥分发和密码应用体系的安全通信产品解决方案，其核心特点为使用量子力学特性生成的量子随机数密钥加密通信数据，对语音、消息等数据进行加密，为移动无线终端场景提供轻量化低成本的量子融合加密的解决方案[14]。

结合运营商加密通信需求，本文基于IMS网络、量子密钥，提出量子加密通信技术架构（见图1）。

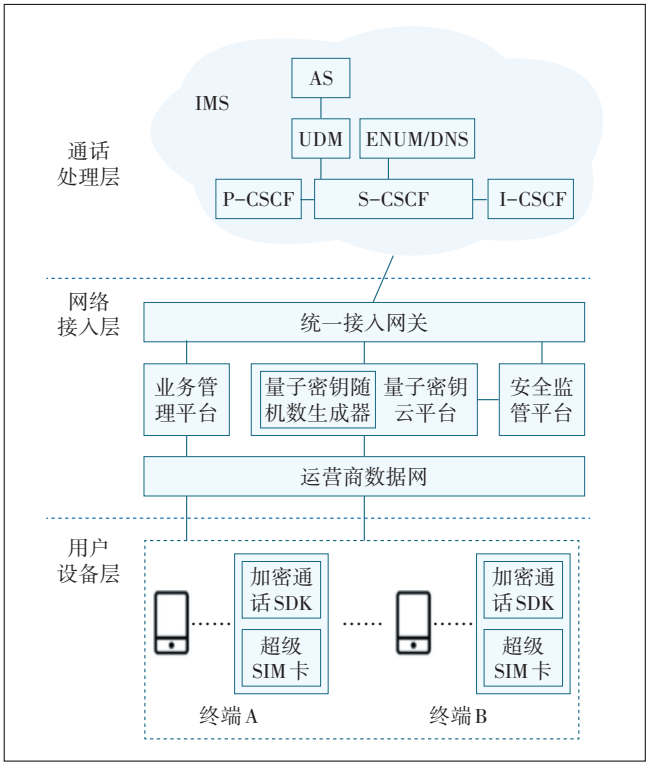

图1　运营商量子加密通信架构

如图1所示，运营商量子加密通信架构分为用户设备层、网络接入层、通话处理层。

用户设备层为嵌入加密通话SDK模块和超级SIM卡的IMS安全终端。在通信时，用户设备层通过网络接入层的业务管理平台、密码服务进行业务处理，借助数据网、统一接入网关与通话处理层互通。其中，IMS终端为嵌入加密通信模块的终端，适用于手机、平板、智能穿戴设备等移动场景及IP话机等固定场景，可为原生IMS终端或通过IMS应用客户端实现。加密通话SDK在前端界面中进行展示并处理用户收发的通信信息，将其交由内置的加密通话模块；加密通话模块利用超级SIM卡与量子密钥云平台预先离线充注的保护密钥，向量子密钥云平台协商获取业务密钥，实现对传输数据的端到端量子加密通信。

网络接入层为此架构的核心定制化部分，由数据网、业务管理平台、量子密钥云平台、安全监管平台、统一接入网关组成，处理来自用户设备层量子加密请求、管理业务开通状态、日志及系统信息，执行身份认证、密钥分发、呼叫控制、通信数据稽查。具体功能如下。

a）运营商数据网：提供IMS终端的移动互联网接入和通信的网络和数据传输服务。

b）业务管理平台：负责加密通信用户业务开通状态合法性校验、通信数据管理等操作。

c）量子密钥云平台：提供基于国密算法加密的身份初始化/周期认证、保护密钥校验、业务密钥分发等功能，结合业务场景加解密用户数据。此外，量子密钥随机数生成器负责对超级SIM卡进行量子密钥充注，提供加密通信保护密钥。

d）安全监管平台：支持依据监管及业务安全要求，对加密通信业务数据进行解密处理，提供实时监管服务。

e）统一接入网关：检测并传输用户的加密通信数据，依据加密业务标识，接入IMS核心网，转发加密及通信请求。

通话处理层为IMS网络架构的业务处理中心，由IMS网络网元构成，通过对现有网元进行配置，实现IMS网络加密通话识别、路由转发、网络互通。IMS网络包含P-CSCF、S-CSCF、I-CSCF、UDM、AS、ENUM/DNS等网元。其中，P-CSCF作为终端信令接入点，负责消息分发、QoS及资源控制；I-CSCF负责匹配选择合适的服务节点，在跨域通信时对底层拓扑结构进行隐藏；S-CSCF负责用户注册鉴权与会话控制，识别、维护呼叫状态，并确保加密通信交互过程的正常开展；UDM负责集中存储用户识别、路由及业务订阅数据；AS负责扩展基础通信能力，为架构提供增值应用；ENUM/DNS负责地址映射和域名解析，为加密通信用户进行全局寻址[15-16]。

本文所提出的技术架构的业务交互流程为：开通加密通信业务的IMS终端通过内置加密通话SDK向业务管理平台、量子密钥云平台分别校验双方的业务开通状态以及身份认证，审查通过后，发起方加密通信

SDK通过统一接入网关向IMS网络发起加密通信请求。IMS网络接收请求并通过加密业务标识、S-CSCF、ENUM/DNS网元完成被叫路由寻址，被叫用户接收请求并返回响应。主被叫双方利用超级SIM卡中的保护密钥加密通信标识，向量子密钥云平台申请业务密钥，保护密钥协商成功后，云平台将密钥分发给用户侧，主被叫使用该业务密钥对媒体包进行加密。IMS网络负责透传加密媒体包，并将其发送给接收方，接收方对加密数据进行解密处理以完成加密通信。该架构通过IMS网元的业务扩展能力与业务管理服务、加密服务的深度融合，有效提升了运营商网络媒体通信的安全性与数据完整性。

3 基于IMS体制的加密通信业务流程

3.1 基于非证书体系的身份认证

为确保加密通信接入安全，本文提出一种非证书认证方案（见图2）。该方案利用国密算法（SM系列）对SIM卡标识与认证密钥进行加密，生成身份认证随机数串，实现用户接入加密通信前的身份认证。

3.1.1 业务开通数据同步

如图2步骤①~④所示，营账侧进行业务开通，开通成功后，将开通业务的号码、超级SIM卡ICCID信息以及绑定关系发送给业务管理平台、量子密钥云平台、IMS UDM、AS网元。

3.1.2 业务管理服务认证

如图2步骤⑤~⑦所示，用户发起加密通信前，通过加密通信终端/APP输入开户号码，终端向业务管理平台发起认证请求。平台校验号码合法性，若号码已开通加密通信服务，则下发加密通信配置文件并返回认证成功响应；若未开通，则返回认证失败信息。

3.1.3 密码服务认证

如图2步骤⑧~⑩所示，通过业务管理服务校验后，终端向量子密钥云平台发起认证请求。终端读取SIM卡内的零号认证密钥与ICCID，使用SM3算法对ICCID信息与认证密钥进行加密，生成哈希值。为防止重放攻击，加密通信SDK模块生成16字节随机数rand1，与哈希值的后16字节拼接，形成唯一的32位认证数据X，终端将X和业务号码发送至密码服务。密

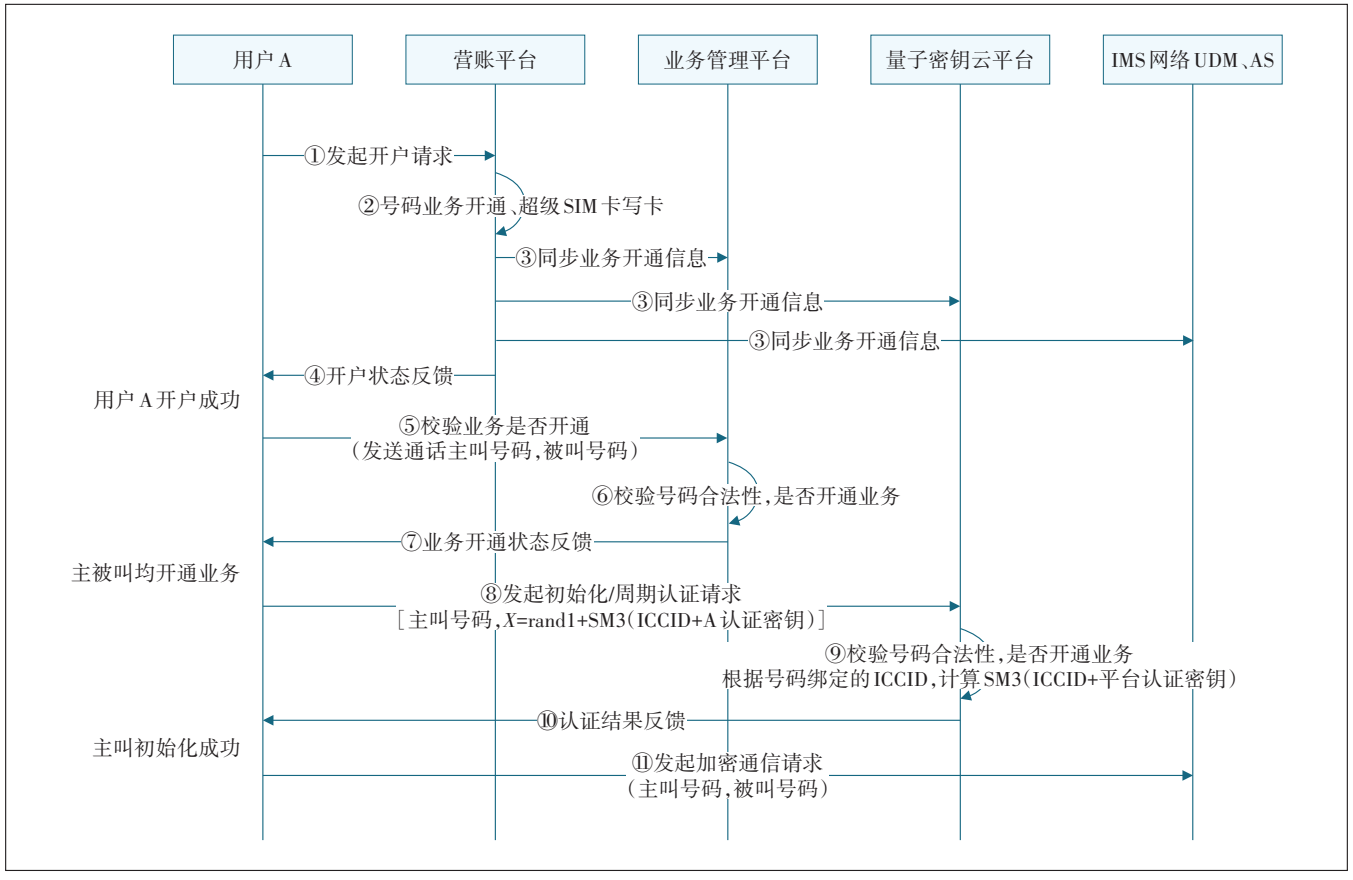

图2 非证书体系的身份认证

码服务通过号码绑定的ICCID与平台零号认证密钥计算对应哈希值，并与终端发送的X的后16位进行比对。比对一致，则认证通过，并发起加密通信请求；否则返回失败。

3.2 一对一通话

在加密通话中，通信双方依次进行信令协商、密钥协商与媒体流加密传输，详细流程如图3所示。

3.2.1 信令协商

如图3步骤①~⑦所示，发起方通过加密通信终端发送加密通话的INVITE请求，VoLTE网络根据业务标识与号码信息寻找到接收方路由，并向接收方发送通话申请。接收方接听后，向发起方返回200 OK信令，确认通话建立，双方进入加密通信阶段。

3.2.2 业务密钥协商

如图3步骤⑧~⑨所示，通话建立后，发起方与接收方通过加密通信SDK向密码服务模块发起密钥协商请求。SDK从SIM卡中随机选取由密码服务生成并预置的保护密钥，结合号码信息、ICCID与VoLTE网络生成的CallID进行加密，形成协商请求。密码服务模块接收后，使用相应的保护密钥解密数据，提取会话ID、号码、ICCID及CallID，并随机生成业务密钥。业务密钥经保护密钥加密后发送至通信双方SDK。双方终端解密获取业务密钥，用于后续媒体数据的加密与解密。

3.2.3 加密媒体流传输

如图3步骤⑩~⑪所示，信令协商与密钥协商完成后，通话双方使用业务密钥对VoLTE网络中RTP包的包体部分进行加密，确保媒体数据安全传输。RTP包头部分保持不变，以便VoLTE网络正常识别与传输。接收方收到加密的RTP包后，使用相同的业务密钥解密包体，恢复通话内容，完成加密媒体流传递。

3.3 安全监管

为保障通信安全与风险可控，本文设计了安全监测服务模块。该模块通过获取密码服务的密钥，对通信管理服务的数据包进行解密，基于通信元数据、身份信息、内容特征及密钥使用规则对经过统一接入网

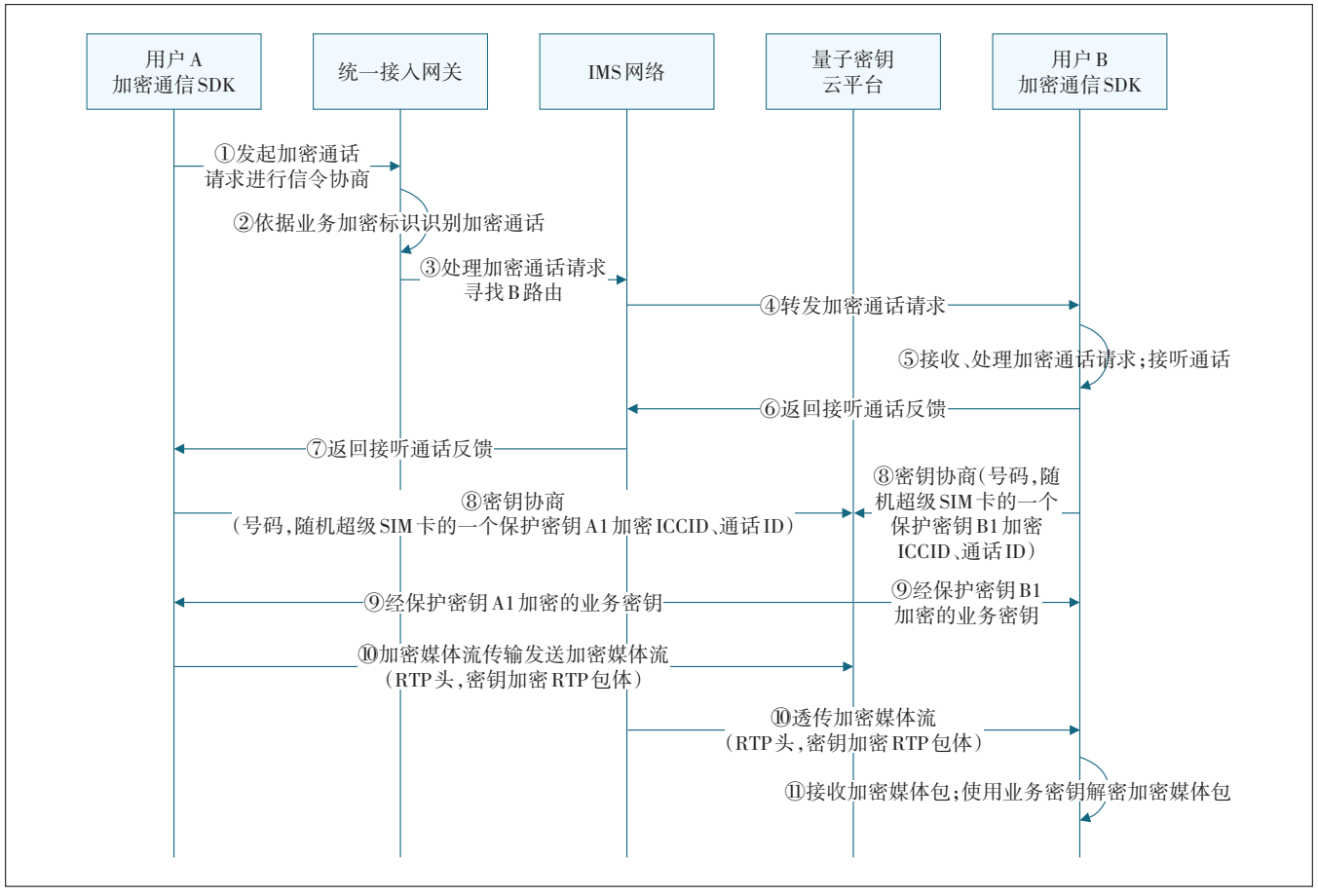

图3　一对一加密通话

关的终端进行监测，提供必要的通话数据、行为分析，判定是否存在加密通信风险。通信数据安全监管示意如图4所示。

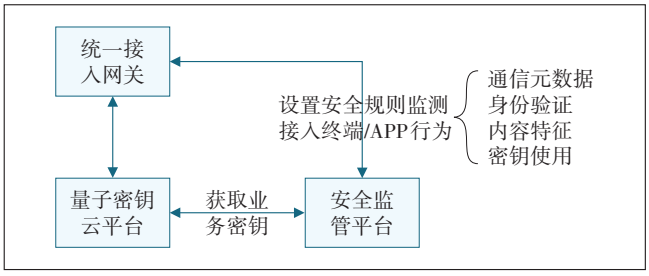

图4 通信数据安全监管

a）基于通信元数据的规则如下。

（a）通信频率规则：监测用户在单位时间内的通信请求数量，标记高频通信的用户，判定阈值为T。

（b）地理位置异常规则：比对通信双方位置，若短时间内位置跨度异常，则标记为异常通信。

b）基于身份验证的规则如下。

（a）多次失败规则：监测用户多次密钥请求的验证结果，若失败次数超出阈值，触发限制机制，暂停密钥分发。

（b）未注册终端规则：对非授权设备或未开户用户自动阻断密钥协商与加密请求，并记录相关信息。

c）基于内容特征的规则为关键词过滤规则。该规则通过解析通信内容，对涉及敏感关键词或特定数据模式的通信实施重点标记与监控。

d）基于密钥使用的规则为密钥唯一性规则。该规则监测业务密钥的使用次数，超过设定阈值的密钥将触发设备与用户分析，当发现重复使用时，停止密钥分发并发出风险告警。

通过上述规则，安全监测服务可有效识别潜在加密通信风险，为通信安全提供精细化管理与多场景保障。

4 总结

本文结合移动通信业务安全需求，提出了运营商网络的量子加密通信技术架构，设计了身份认证、一对一加密通话、安全监管等关键业务流程。该架构基于加密通信SDK、密码服务、加密通信业务管理平台和安全监管平台，旨在构建更加安全可靠的基础语音通信解决方案，满足用户对高等级通信安全的需求。随着6G网络的普及和用户安全通信需求的增长，基于量子密钥分发技术的加密通话、数据通信、短消息等解决方案将逐步落地，并广泛应用于政府、国防、金融等保密性较高行业的安全通信场景。

参考文献：

[1] 宋安平，高新平，王静，等. 基于量子安全加密技术的5G通信创新应用[J]. 江苏通信，2022，38(4)：74-78.
[2] 李建华，银鹰，李思源，等. 大数据安全与隐私计算技术综述[J]. 网络空间安全科学学报，2024，2(6)：1-15.
[3] 苗春华，王剑锋，魏书恒，等. 基于量子密钥的移动终端加密方案设计[J]. 网络安全技术与应用，2018(6)：38，44.
[4] 黄晓平. 量子密钥分发技术在计算机网络安全中的应用[J]. 网络与信息，2024，36(19)：126-128.
[5] 运行监测协调局. 2025年通信业统计公报[EB/OL]. [2026-01-29]. https://wap.miit.gov.cn/gxsj/tjfx/txy/art/2026/art_5c99d65350f7452f999e8efcb1ee2d6a.html.
[6] PALAMÀ I，GRINGOLI F，BIANCHI G，et al. IMSI catchers in the wild：a real world 4G/5G assessment[J]. Computer Networks，2021，194：108137.
[7] 胡鑫鑫，刘彩霞，彭亚斌，等. 5G鉴权认证协议的安全性研究[J]. 无线电通信技术，2020，46(4)：405-411.
[8] 黄文，薛宁波，梁小洁，等. 通信运营商防控网络运营风险的有效路径分析[J]. 网络安全技术与应用，2024(3)：100-102.
[9] 李健. 移动计算环境中的网络安全防护策略分析[J]. 电子技术，2024，53(3)：314-315.
[10] 冯亮. 基于移动通信技术的信息安全技术研究[J]. 通信电源技术，2020，37(11)：221-223.
[11] 庄仁峰，黄伟湘，黄健文，等. 移动认证：基于运营商通信网络的统一身份认证技术[J]. 网络空间安全，2022，13(6)：63-68.
[12] 刘春蕾. IMS在通信领域的应用与前景分析[J]. 数字化用户，2018，24(28)：23，230.
[13] 郎睿. IMS网络与现网业务融合探讨[J]. 中国新通信，2023，25(10)：58-60.
[14] 吴洪祥，李欣刚，叶国林. 基于SM2和后量子密码的融合密钥协商的应用与探索[J]. 数字技术与应用，2024，42(2)：97-99.
[15] 李秀全. IMS应用及存在的问题探讨[J]. 数字化用户，2019，25(43)：8.
[16] 廖蓉晖，张鹤鸣，许志强. 基于IMS的VoIP系统加密体制研究[J]. 网络安全技术与应用，2024(9)：38-40.

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；梁艳，高级工程师，博士，主要从事通信网络前瞻研究和方案规划工作。