基于VoLTE的新型轻量化量子加密通话方案研究

Research on New Lightweight Quantum-Encrypted Call Scheme Based on VoLTE

马长链，杜忠岩，冷 超（中国联通智能城市研究院，北京 100048）
Ma Changlian，Du Zhongyan，Leng Chao（China Unicom Smart City Research Institute，Beijing 100048，China）

摘 要：
VoLTE通过将语音数据流与普通数据流同时承载于通信运营商的LTE网络上，实现数据业务与语音业务在同一网络下的统一承载，成为了通信行业公认的语音业务最佳承载方案。为了给高等级用户提供更安全的VoLTE服务，通信运营商提出了基于VoLTE的量子加密通话技术。然而，传统的实现方案需要改造IMS网络和手机芯片，过程非常复杂且无法实现跨运营商的量子加密通话。基于对VoLTE语音通话具体流程的分析，提出了一种新型轻量化实施方案。

关键词：
量子加密；VoLTE；安全通话；量子加密通话
doi：10.12045/j.issn.1007-3043.2025.11.016
文章编号：1007-3043（2025）11-0082-06
中图分类号：TN918
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
By transmitting both data information and voice information on the LTE network of the telecom operator，the data service and voice service are carried under the same network，VoLTE becomes the best voice service carrier recognized by the communication industry. In order to provide more secure VoLTE service for high level users，telecom operators have proposed the quantum-encrypted call technology based on VoLTE，but the traditional implementation method needs to upgrade the IMS network and the mobile phone chip，and the process is very complicated and can not realize the quantum-encrypted call across different telecom operators. Based on the analysis of the specific voice call process of VoLTE，a new lightweight implementation scheme is proposed.

Keywords：
Quantum encryption；VoLTE；Secure call；Quantum-encrypted call

引用格式：马长链，杜忠岩，冷超. 基于VoLTE的新型轻量化量子加密通话方案研究[J]. 邮电设计技术，2025（11）：82-87.

1 信息安全需求分析及发展现状

在信息时代，小到个人交流、中到日常办公、大到国际事件，无时无刻不在产生数据信息，但是现有安全体系却无法完美保障信息的安全[1-2]。另外，量子计算机的快速发展，也给现有经典密码体系带来了巨大的挑战。信息安全主要考虑3个层面，即攻不进、拿不走、破不开，“破不开”是用密码技术来进行保障的最后一道安全防线，而密码技术的核心就是密钥的产生。根据香农信息论，密钥真随机产生、不能重复使用、不少于明文长度才能实现无条件安全[3]。当前的加密体系在密钥“产生”方面存在一定的短板。量子具有测不准、不可克隆、不可分割三大特性，也就决定了量子密钥具有真随机、不可预测、不可复制的特性，因此，基于量子特性产生的量子密钥，在增强当前加密体系方面具有非常突出的优势。融合量子密钥与传统安全技术的量子加密通信技术，具有数学上无法被窃听和破解的绝对安全保证，是很好的信息安全解

收稿日期：2025-09-12

决方案[4-12]。

为了满足高等级用户对通话安全的要求，通信运营商以及相关手机通信厂商将量子加密通信技术与VoLTE（Voice over Long-Term Evolution）技术相结合，提出了基于VoLTE的高清量子加密通话（简称“VoLTE量子密话”）服务。2022年，通信运营商A发布了通信行业内首款基于量子加密技术的VoLTE加密通话终端产品，该终端产品采用了国产化定制手机、量子安全SIM卡以及国密算法。同年，通信运营商B将量子密码技术与VoLTE加密通话相结合，提出了基于量子密钥的VoLTE加密通话系统技术方案，该系统主要由量子密码安全服务中心、VoLTE通信系统、专用手机终端以及量子密码卡组成。2023年，某通信厂商推出了一款全新量子密话定制版手机，这款手机采用国产芯片、国密算法和量子安全SIM卡，具备量子密话功能。

目前，通信运营商以及手机终端厂商实现VoLTE量子密话的主流方案是扩展SIP协议字段，并启用附带预置条件的呼叫会话流程。该技术方案需要对现有的IMS网络进行改造，改造后的IMS网络需要对SIP扩展字段采用默认的透传方式。另外，为了适配IMS网络侧的改造，手机终端侧的Modem芯片系统也需要进行改造，以识别接收到的SIP扩展字段，并对SIP扩展字段的内容进行解析处理。然而，该VoLTE量子密话方案存在IMS整网改造协调难度大、投入成本高、建设周期长，需要芯片厂商和手机终端厂商的配合，以及无法跨通信运营商网络进行VoLTE量子密话等问题。

针对以上问题，本文提出了一种在不改造IMS网络、SIP协议、Modem芯片的前提下，实现全网VoLTE量子密话的新型轻量化技术方案。

2 基于VoLTE的高清量子加密通话架构分析

基于VoLTE的高清量子加密通话主要包括3个部分，分别是通信运营商提供的VoLTE服务、量子密钥中心以及手机终端，三者之间的逻辑架构如图1所示。

其中，通信运营商LTE网络负责提供VoLTE语音网络和服务，当手机终端侧对语音流进行量子加密以后，VoLTE语音网关能够正常透传该加密语音流；量子密钥中心用于识别合法手机终端的安全接入，进行手机终端的管理、注册、身份认证等工作，并对量子密钥的产生、存储、分发等全生命周期进行管理[13]；手机终端集成了量子加解密模块，用于对数字语音流进行量子加密，量子加解密模块支持SM2、SM4等国密算法[14]，同时，量子加解密模块实现手机终端到量子密钥中心的注册、安全接入和密钥协商功能。在具体实践中，量子加解密模块的载体可以是TF卡、超级SIM卡、手机上的存储区或者集成于手机主板上的安全芯片[15]等。

3 VoLTE量子密话加解密流程分析

3.1 普通VoLTE语音通话过程

普通VoLTE语音通话流程如图2所示[16]。

VoLTE语音通话发送语音环节的语音传递流程如下。

a）手机的麦克风捕获到语音模拟信号，并转化为原始数字语音信号。

b）Codec的编码算法模块对原始语音信号进行编码，并通过声码器提取编码语音特征值。

c）语音特征值经Modem调制为模拟信号，并发射出去。

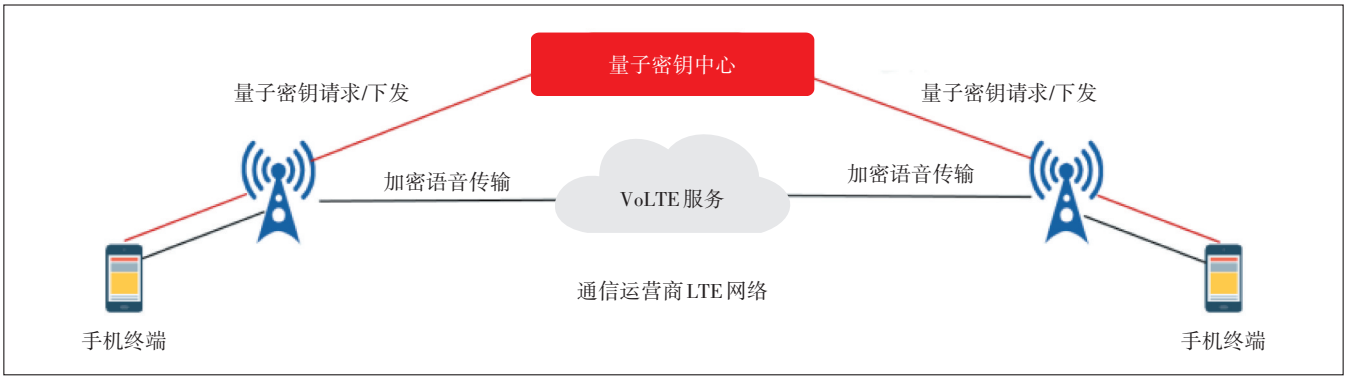

图1　基于VoLTE的高清量子加密通话原理架构

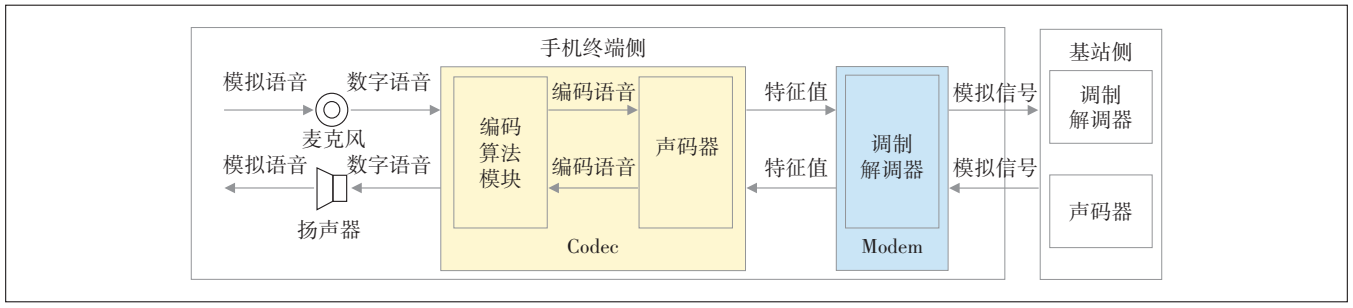

图2 VoLTE语音通话流程

d）发射出的模拟信号到达基站，基站对模拟信号进行解调并利用声码器将解调信号转换为标准的PCM语音流，而后进入核心交换网络进行传输。

VoLTE语音通话接收语音环节的语音传递流程如下。

a）经过核心交换网络的标准PCM语音流到达基站后，通过基站的声码器处理、调制解调器调制后变为模拟信号，并通过基站天线发射出去。

b）手机终端截获模拟信号，Modem将模拟信号解调为数字语音流（语音特征值）。

c）数字语音流（语音特征值）进入Codec，经过声码器处理、编码算法模块解码后，输出语音数字信号，并发送至手机扬声器。

d）扬声器将语音数字信号转化为语音模拟信号并输出。

3.2 主流VoLTE量子密话语音加解密过程

3.2.1 主流VoLTE量子密话系统实现原理

主流VoLTE量子密话语音加解密流程如图3所示。以加密过程为例进行详细分析，该方案在Codec芯片处理之后，语音数据特征值进入Modem芯片之前，增加量子加解密模块，实现对语音数据特征值的量子加密。此时语音信号已经数字化，变换的质量和安全性都更高。但是，该方案的实现过程较为复杂，涉及诸多改造工作，具体如下。

a）改造信令控制协议——SIP协议。扩展SIP协议字段，将手机终端进行VoLTE量子密话的“加密标识”携带在SIP请求呼叫Call-Info头的generic parameter扩展字段。

b）改造IMS网络。当VoLTE量子密话终端发起建立量子密话指令时，将“加密标识”携带在SIP扩展字段，且需要整个IMS网络能够透传该扩展字段，故需要对IMS网络进行改造。

c）改造手机端Modem芯片。主流VoLTE量子密话的“语音加解密功能实现”是在Codec芯片处理之后、语音数据特征值进入Modem芯片之前进行，故需要在Modem芯片中植入量子加解密模块，同时，需要对Modem芯片系统进行改造，使Modem芯片具备识别SIP扩展字段内容、对语音数据特征值进行量子加解密这2个功能。

另外，该技术方案需要手机终端方面的系统支持，如提供底层接口及协议、系统设置相关的UI修改等。

3.2.2 主流VoLTE量子密话劣势分析

如前文所述，该方案需要对通信运营商的现有

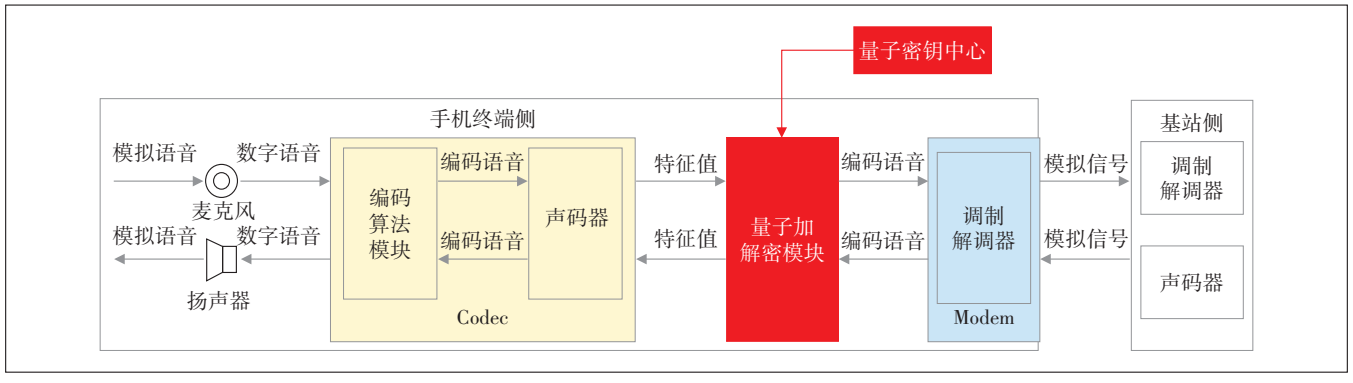

图3 主流VoLTE量子密话语音加解密流程

IMS网络进行整体改造，协调难度大、投入成本高、建设周期长，存在潜在的不可预知、不可控因素，影响现网业务。同时，该方案需要芯片厂商和手机终端厂商的配合，Modem芯片和手机终端均需要定制。另外，对于不同的通信运营商，受各自IMS网络改造需求的制约，网络制式不尽相同，无法实现跨通信运营商的VoLTE量子密话，如以下2种情况。

a）运营商A进行了SIP扩展字段改造和IMS网络改造，运营商B未进行任何改造。

b）运营商A和运营商B均进行了SIP、IMS网络改造，但是运营商A携带在SIP扩展字段的“加密标识”与运营商B携带在SIP扩展字段的“加密标识”不同。

基于以上分析，探索新型轻量化的VoLTE量子密话语音加解密方案是十分必要的。

3.3 新型轻量化VoLTE量子密话语音加解密方案

3.3.1 新型轻量化VoLTE量子密话系统实现原理

针对主流VoLTE量子密话方案存在的问题，本文提出了新型轻量化VoLTE量子密话方案，在普通VoLTE语音通话基础上，新增“语音编解码及量子加解密模块”这一核心模块，该模块由“语音编解码算法”和“量子加解密算法”2个子模块构成。其中，语音编解码算法子模块的主要功能是语音过滤、噪声剔除、人声提取、语音编解码等；量子加解密算法子模块的主要功能是实现对编码语音的量子加解密，同时实现支持国密算法、量子密钥协商等功能。

本方案的语音加解密流程如图4所示。本方案的核心思想是对麦克风输出的数字语音信号进行“语音特征值提取+量子加密”变换，且变换后得到的数字语音密文符合Codec芯片对语音信号的特征要求，手机接收端通过逆运算来合成原始语音。在具体实践中，因变换操作会或多或少对原始数字语音信号造成不可逆丢失，故还原的语音质量可能有不同程度的受损，但并不影响声音的舒适感和对通话内容的准确理解。

3.3.2 新型轻量化VoLTE量子密话语音传递流程分析

新型轻量化VoLTE量子密话发送语音环节的语音传递流程如下。

a）手机终端麦克风捕获到语音模拟信号，并转化为原始数字语音信号。

b）语音编解码及量子加解密模块中的语音编码算法提取数字语音信号的语音特征值，量子加密算法将数字语音的语音特征值加密成“数字语音密文”输出至Codec芯片。

c）Codec芯片利用编码算法模块将数字语音密文输出为编码语音密文。

d）编码语音密文拥有语音特征，可以通过声码器特征提取要求，声码器提取得到“数字语音密文”的特征值。

e）声码器处理后的特征值，经Modem调制为模拟信号，并发射出去。

f）发射出的模拟信号到达基站，基站对模拟信号进行解调并利用声码器将解调信号转换为标准的PCM语音流，再进入核心交换网络进行传输。

新型轻量化VoLTE量子密话接收语音环节的语音传递流程如下。

a）经过核心交换网络的标准PCM语音流到达基站后，通过基站的声码器处理、调制解调器调制后变为模拟信号，并通过基站天线发射出去。

b）手机终端截获模拟信号，Modem将模拟信号解调为数字语音流（语音特征值）。

c）数字语音流（语音特征值）进入Codec，经过声码器处理后得到加密的数字语音数据，即编码语音密

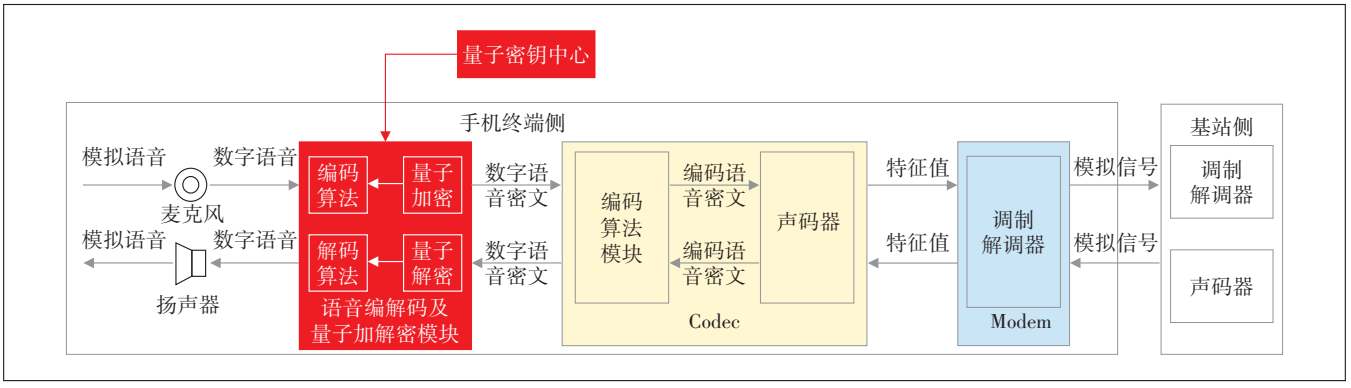

图4　新型轻量化VoLTE量子密话语音加解密流程

文。

d) 编码语音密文经过Codec的编码算法模块解码之后,得到量子加密的“数字语音密文”。

e) 语音编解码及量子加解密模块对“数字语音密文”进行量子解密,得到由发送方原始数字语音信号变换后的语音特征值,语音解码算法对语音特征值进行逆运算,得到发送方的原始语音数字信号。

f) 扬声器将原始语音数字信号转化为语音模拟信号并输出。

3.3.3 新型轻量化VoLTE量子密话量子加密过程解析

本文提出的新型轻量化VoLTE量子密话,通过注册、量子密钥下发、VoLTE通话加密3个步骤,可在不同的手机终端之间实现VoLTE量子密话。注册、量子密钥下发、VoLTE通话加密这3个步骤的详细过程如图5所示。其中,手机终端唯一标志是指手机终端的IMEI码;量子会话密钥是指由量子密钥中心生成,用于不同手机终端之间通话语音流加密的量子密钥;身份认证密钥是指离线充注到手机终端中的密钥(具体充注载体可以是TF卡、超级SIM卡、手机上的存储区、集成在手机主板上的安全芯片等),用于进行手机终端合法用户身份认证,量子会话密钥的加密下发等。

采用超级SIM卡作为手机终端侧量子加解密模块的硬件载体,并以此为例,对VoLTE量子密话业务的量子加密过程进行进一步解析。

a) 手机终端用户注册上线。手机终端用户A和手机终端用户B使用超级SIM卡预充注量子密钥作为身份认证密钥,注册成功并上传唯一标志码和本机号。

b) 量子会话密钥下发。在拨打电话时,手机终端用户A(主叫方)告知量子密钥中心手机终端用户B(被叫方)的号码,量子密钥中心使用预充注的量子密钥,即身份认证密钥,对量子会话密钥加密后,下发给手机终端用户A和手机终端用户B。

c) VoLTE通话加密。手机终端用户A和手机终端用户B分别使用预充注的量子密钥(身份认证密钥)进行解密,得到量子会话密钥,并用量子会话密钥保护VoLTE通话的语音数据流,从而实现基于VoLTE的高清量子加密通话。

4 新型轻量化VoLTE量子密话方案优势分析

首先,该方案可安全、可靠、便捷地实现VoLTE量子密话。新型轻量化VoLTE量子密话与主流VoLTE量子密话技术方案特点对比如表1所示。由表1可知,与主流VoLTE量子密话相比,新型轻量化VoLTE量子密话具有不改造IMS网络、SIP协议、Modem芯片,方案实现简单,成本较低,开发周期较短的优势。结合量子加密的一话一密等特性,可安全、可靠、便捷地实现VoLTE量子密话。

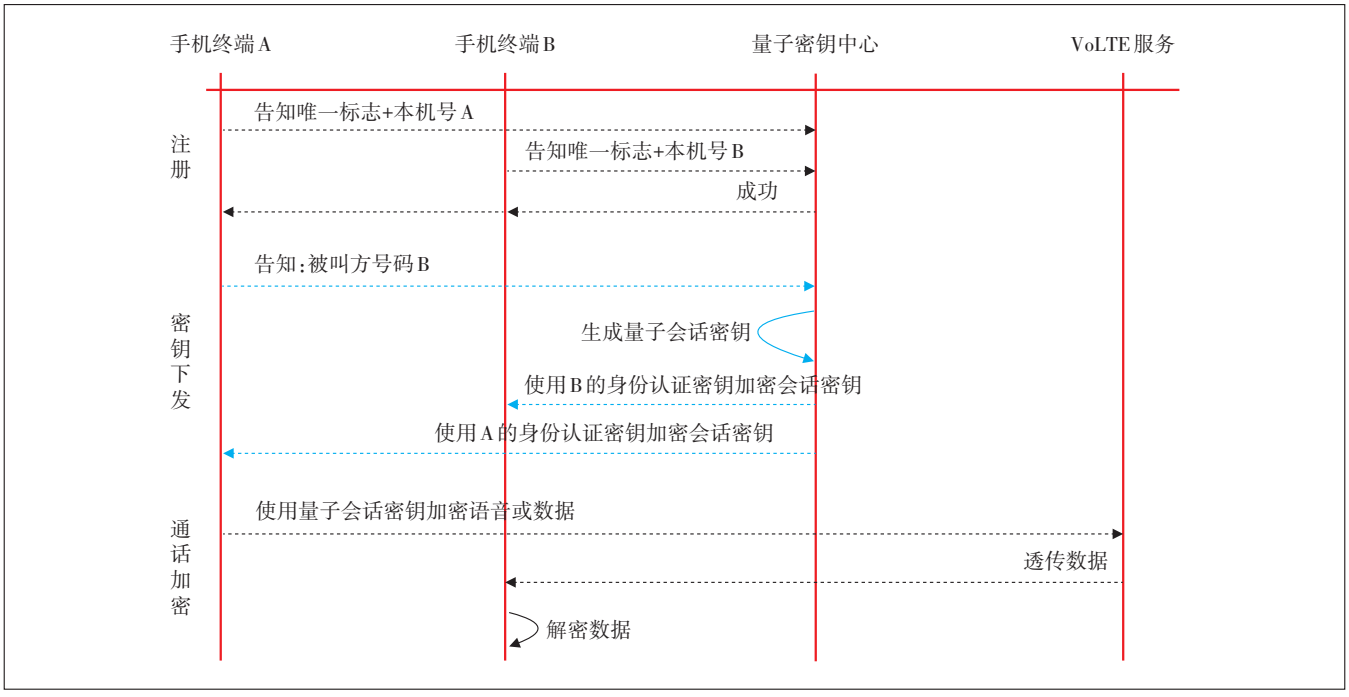

图5 新型轻量化VoLTE量子密话实现过程

表1　新型轻量化VoLTE量子密话与主流VoLTE量子密话技术方案特点对比

序号	对比内容	新型轻量化VoLTE量子密话		主流VoLTE量子密话	
		是/否	说明	是/否	说明
1	是否需要修改IMS网络	否	-	是	网络需支持透传SIP扩展字段
2	是否需要修改SIP协议	否	-	是	需扩展SIP协议字段
3	是否需要改造手机芯片	否	-	是	芯片需识别SIP扩展字段；同时增加量子加解密功能模块
4	是否需要手机端厂商配合	是	手机需定制，系统需支持加解密流程；同时增加量子加解密功能模块	是	手机需定制，系统需支持加解密流程
5	是否支持跨运营商VoLTE量子密话	是	-	否	不同运营商IMS网络改造不同，VoLTE量子密话不可互通

其次，该方案支持不同形态的硬件载体，兼容多种密码算法。在具体实践中，新型轻量化VoLTE量子密话方案支持手机终端侧采用不同形态的硬件载体来承载语音编解码及量子加解密模块，如TF卡、超级SIM卡、手机上的存储区、与手机主板集成在一起的安全芯片等。此外，该方案支持国密算法（如SM2、SM4），支持定制灌入客户的语音编码算法以及量子加解密算法。

最后，量子会话密钥可保障VoLTE量子密话全过程的语音数据安全。量子密钥中心具有完备的量子会话密钥存储、分发、更新等安全机制，量子会话密钥的真随机、不可预测特性可保障VoLTE量子密话全过程的语音数据安全传输。同时，可根据实际需求，通过在手机终端存储载体中预置量子会话密钥的方式实现VoLTE量子密话。

5 总结

本文介绍了通信运营商提出VoLTE量子密话服务的背景，以及VoLTE量子密话技术架构中VoLTE服务、量子密钥中心、手机终端这三大要素各自的功能以及相互之间的逻辑关系。从实践角度出发，本文分析了主流VoLTE量子密话语音加解密过程的技术实现方法，并对主流实现方法面临的问题进行了充分的剖析。考虑到主流VoLTE量子密话语音加解密实现过程的复杂性，本文提出了新型轻量化VoLTE量子密话技术方案，并对新型轻量化VoLTE量子密话在实现过程中涉及的手机终端注册、量子密钥下发、VoLTE通话加密3个关键步骤进行了充分的论述。新型轻量化VoLTE量子密话方案可以安全、可靠、便捷地实现VoLTE量子密话，支持不同形态硬件载体、兼容多种密码算法，能够对量子会话密钥进行安全分发、存储、更新等生命周期管理，具有一定的推广应用价值。

参考文献：

[1] 李兴新，郭晓花，侯玉华，等. 新形势下移动终端安全需求和对策[J]. 邮电设计技术，2021(6)：88-92.
[2] 赵晓松. 移动智能终端的安全威胁分析[J]. 济南职业学院学报，2020(3)：119-121.
[3] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal，1949，28(4)：656-715.
[4] 冷超，杜忠岩，王题，等. 量子保密通信技术及其在智慧城市中的应用研究[J]. 邮电设计技术，2023(4)：33-37.
[5] 赖俊森，吴冰冰，汤瑞，等. 量子通信应用现状及发展分析[J]. 电信科学，2016，32(3)：123-129.
[6] 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.
[7] 许伟. 量子保密通信技术应用及未来发展分析[J]. 信息技术与信息化，2020(3)：92-94.
[8] 程明，张成良，唐建军. 量子保密通信应用与技术探讨[J]. 信息通信技术与政策，2022(7)：14-19.
[9] 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.
[10] 谢小兵. 量子密码技术原理及应用前景初探[J]. 金融电子化，2021(7)：64-66.
[11] 郭光灿. 量子信息技术研究现状及未来[J]. 中国科学(信息科学)，2020，50(9)：1395-1406.
[12] 王斌，李进珍. 基于量子加密移动视频系统实现与应用[J]. 网络安全和信息化，2020(10)：123-126.
[13] 杜忠岩，冷超，王题，等. 面向5G网络的量子加密在智慧城市中的应用[J]. 邮电设计技术，2022(5)：16-21.
[14] 李子臣. 商用密码算法原理与C语言实现[M]. 北京：电子工业出版社，2020.
[15] 陈格. 一种基于安全芯片的VoLTE加密通话方案设计与实现[D]. 重庆：重庆邮电大学，2017.
[16] 江林华. LTE语音业务及VoLTE技术详解[M]. 北京：电子工业出版社，2016.

作者简介：
马长链，毕业于北京邮电大学，高级工程师，硕士，主要从事量子加密通信、北斗定位、工业互联网等技术研究工作；杜忠岩，毕业于华中科技大学，教授级高级工程师，硕士，主要从事移动通信、北斗定位、智慧城市等技术研究工作；冷超，毕业于南京邮电大学，高级工程师，学士，主要从事量子通信、智慧城市等技术研究工作。