面向5G网络的量子加密在智慧城市中的应用

Application of Quantum Cryptography for 5G Network in Smart City

杜忠岩[1]，冷　超[1]，王　题[1]，黄大骏[2]（1. 中国联通智能城市研究院，北京 100033；2. 浙江九州量子信息技术股份有限公司，浙江 杭州 311201）

Du Zhongyan[1], Leng Chao[1], Wang Ti[1], Huang Dajun[2]（1. China Unicom Smart City Research Institute, Beijing 100033, China; 2. Zhejiang Jiuzhou Quantum Technologies Co., Ltd., Hangzhou 311201, China）

摘　要：

随着5G无线网络的发展，影响无线网络安全的因素也越来越多，其相关应用正面临着信息安全问题。针对无线网络的安全现状，量子通信技术具备无条件安全的特性，是未来智慧城市各场景应用安全防护的重要对策。介绍了面向5G无线网络的量子密钥分发技术，并论述了量子加密在智慧城市相关领域的创新应用，最后探索量子加密技术与5G网络融合的安全研究应用前景。

关键词：

5G；无线网络；密钥分发；量子密钥云平台

doi：10.12045/j.issn.1007-3043.2022.05.004

文章编号：1007-3043（2022）05-0016-06

中图分类号：TN929.5

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the development of 5G wireless network, there are more and more factors affecting the security of wireless network, and its related applications are facing the problem of information security. In view of the current security situation of wireless networks, quantum communication technology has the characteristics of unconditional security, which is an important countermeasure for application security protection in various scenarios of smart cities in the future. It introduces the quantum key distribution technology for 5G wireless network, discusses the innovative application of quantum encryption in related fields of smart city, and finally explores the security research and application prospect of the integration of quantum encryption technology and 5G network.

Keywords：

5G; Wireless network; Key generator; Quantum key cloud platform

引用格式：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.

1 无线网络安全分析

1.1 无线网络安全现状分析

随着智慧城市的快速发展，相关的信息化技术也在不断更新迭代，5G相关产业正在快速落地，基于5G网络的智慧城市应用对安全防护技术提出了更高的要求。传统网络的数据安全机制一般采用对称加密技术，其在信息交互中未全面考量到无线通信的基本特性，比如在连接建立时的身份认证、传输通道的数据加密、密集网络的密钥管控等方面缺乏有效的安全管理。

1.1.1 开放特性安全

相较于有线网络，无线通信运用开放性信道，便于数据交互的同时也带来了不安全的可能性，导致通信信道上的信令与内容易被窃听、被更改、被假冒。其次，终端侧与无线网络间无物理连接，设备接入随机性高，容易产生欺骗问题。虽然有线网络也存在被

基金项目：国家重点研发计划（2019YFB2103200）

收稿日期：2022-03-25

窃听的隐患，但对于无线网络，黑客通过特定的无线通信设备更容易窃听，而且不容易被发现。

1.1.2 数据传输安全

在无线网络中，当终端侧海量设备建立连接后，将产生大量的数据传输与交互，均存在安全隐患。数据交互涵盖2个方面，一是核心网侧信令及数据的交互，二是接入网侧信令及数据的交互。对于这2个方面的数据交互，黑客都可以开展各种类型的攻击，并从中获利。

1.1.3 终端接入安全

无线网络根据业务需求接入一定数量的移动终端设备，覆盖范围较大，难以全方位地进行安全管理，存在接入侧的安全问题。如果不法分子通过移动终端设备对无线网络链路进行攻击，或者在设备上植入病毒、木马等，将对整个数据链路和业务系统造成影响。

1.1.4 敏感数据安全

在无线网络中，业务系统服务众多，而一些敏感的用户隐私数据和关键业务数据在无线信道传输中易受到黑客攻击。此外，无线网络会涉及第三方网络的开放共享，比如银政数据、政企数据等。若对第三方网络开放一定的权限，面临的安全威胁、信任问题也会更加复杂。

1.2 量子保密通信技术在无线网络中的优势和局限

量子保密通信技术是在量子通信理论的基础上发展起来的，是一种利用量子叠加态和纠缠效应进行信息传递的新型通信方式，具有无法被窃听和无法被计算破解的无条件安全性保证，是保障网络信息安全的有效手段。

在无线网络中，量子通信技术结合了无线通信领域的实际需求，实现了分区分域工作、内外网分离的通信，而且量子技术不会对现有网络拓扑造成影响，可以做到无缝对接，透明加密，满足了成本、性能、可靠性等各方面的综合要求。在智慧城市的各个应用场景中，原有的安全防护措施都可与量子密钥分配技术紧密结合，进而提高业务系统的安全性，如视频会议、集群对讲、无人机巡检等的数据传输场景。图1给出了量子保密通信流程示意。

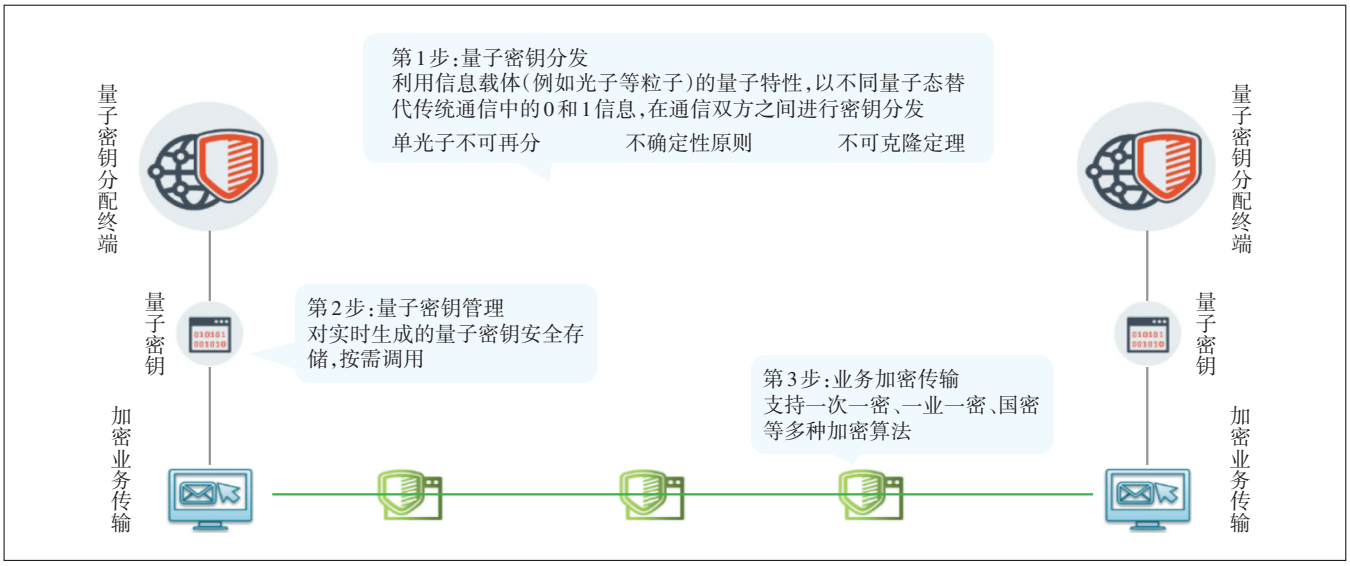

图1　量子保密通信流程示意图

1.3 5G网络中量子加密技术的优势

大规模的量子保密通信网络，会耗费大量的光纤资源，导致量子保密通信网络建设成本高、运维管理难度大，在一定程度上限制了量子保密通信网络的发展。此外，每一次的量子密钥分发都需要至少4次经典信道的信息传递，对量子加密通信的整体效率有一定的影响。

基于5G网络提供量子加密服务不仅可以节约光纤资源，还可以更好地应用到智慧城市各业务场景中，保障网络数据安全，明显提高网络建设的经济效益和社会效益。应用量子加密技术，能够防止数据被修改，大幅提升终端在5G网络中的安全水平。而且，量子加密服务器对外提供的加解密服务和密钥分发服务对原有网络架构不产生影响，应用灵活，易于扩

展,易于部署。

1.4 城市级安全共生系统

面向新一代智慧城市的建设,万物互联,安全在其中的重要性越发显著。未来,服务于智慧城市的城市级安全共生系统将突破传统“信息化系统先建后防护”的安全服务模式,打造城市安全基座及服务能力,提供可定制、可编排的面向全行业、全领域、全生命周期的定制化安全服务。其中量子加密技术将发挥重要作用,为智慧城市提供更有力的安全保障。量子密钥云平台作为量子加密应用的基础,能够提供包括密钥生成、存储、分发等全生命周期的管理能力,城市级安全共生系统架构如图2所示。

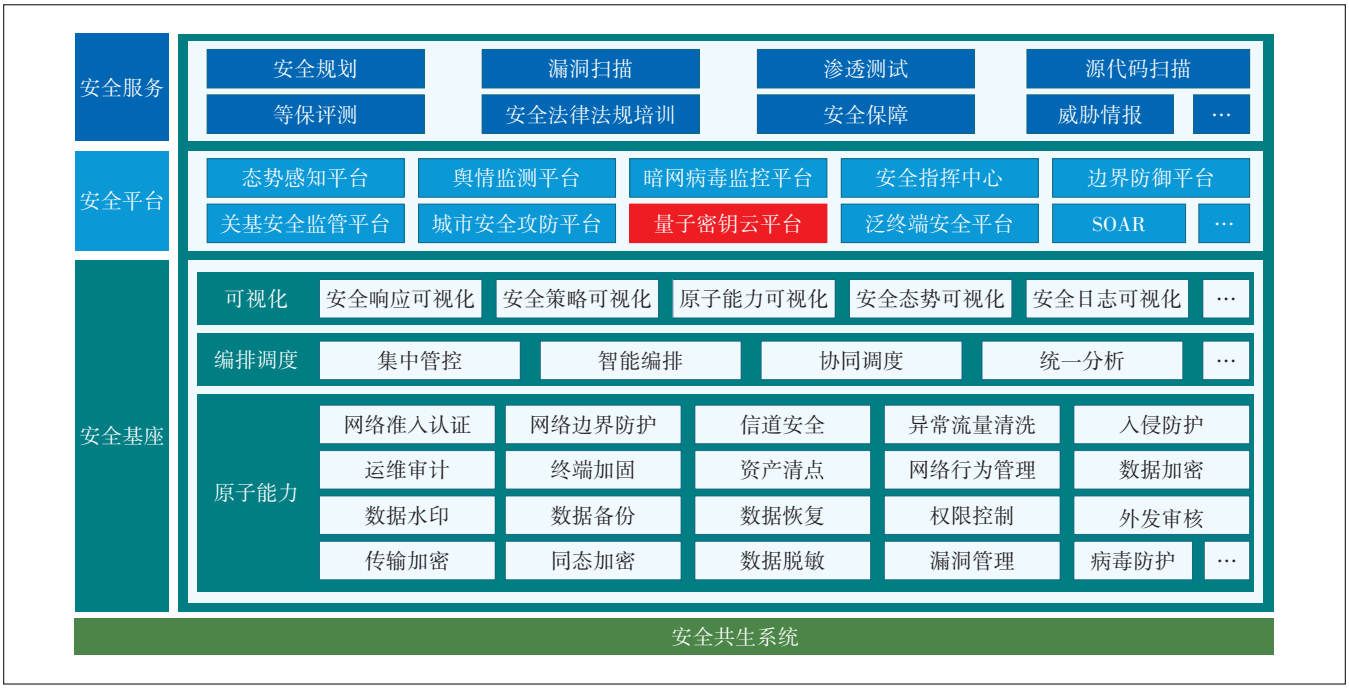

图2　城市级安全共生系统架构

2 面向5G网络的量子加密技术

2.1 量子真随机数生成

在5G无线网络中,为了保障数据安全,可以运用量子随机数发生器作为业务应用的密钥源,其原理是基于激光器的自发辐射的相位波动而产生的真随机数源,其熵源完全来自激光器自发辐射的随机相位波动,经论证其具有理论可证的不可预见性。量子随机数发生器生成的随机数具有良好的统计特性,原理如图3所示。

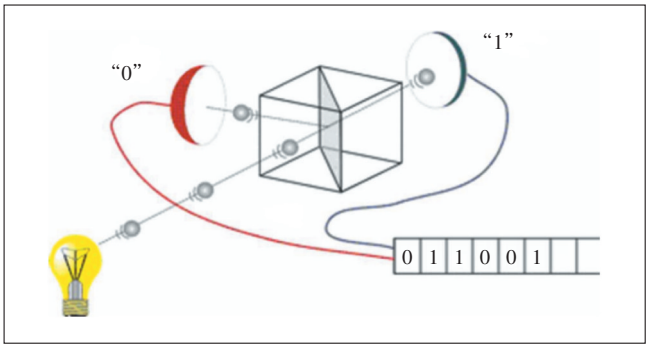

图3　量子真随机原理图

2.2 5G网络终端身份认证

在无线网络的核心网侧,终端与量子密钥云平台,后端平台与量子密钥云平台预置共享一个公共的量子密钥(身份密钥K)。通过身份密钥完成实体间的双向鉴别,具体机制如图4所示。

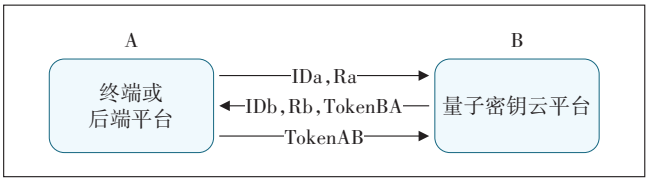

图4　双向鉴别机制图

其中,终端或后端平台简称实体A,量子密钥云平台简称实体B,TokenAB是从实体A发往实体B的鉴别信息,TokenBA是从实体B发往实体A的鉴别信息。

双向身份认证具体流程如下：

a）实体A预置身份密钥K，实体量子加密模块标识IDa，生成随机数Ra，并将IDa和Ra发送给实体B。

b）实体B预置身份密钥K，实体量子加密模块标识IDb，生成随机数Rb。接收实体A发送过来的IDa和Ra，并将IDb、Rb和TokenBA发送给实体A，其中TokenBA = H，H = HMAC(N,K)，N = IDa‖Ra‖Rb。

c）实体A接收实体B发送过来的IDb、Rb和TokenBA，计算HMAC(IDb‖Ra‖Rb,K)，并验证计算结果是否与收到的TokenBA一致，一致则发送TokenAB发送给B，其中TokenAB = H，H = HMAC(N,K)，N = IDa‖Rb‖Ra。

d）实体B接收到实体A发送过来的TokenAB，计算HMAC(IDb‖Rb‖Ra,K)，并验证计算结果是否与收到的TokenAB一致，一致则双向身份认证成功。

身份鉴别协议层报文格式如表1所示。身份鉴别协议报文根据报文类型发送3帧的数据报文，报文类型相应值为0x0080，0x0081和0x0082。

表1　身份鉴别协议层报文

起始标识 2字节	报文长度 2字节	报文类型 2字节	封装数据域 身份鉴别数据	校验和
EAE0				

2.3 量子密钥分发更新

量子密钥更新方面采用终端或平台主动进行更新的方式。终端通过量子加密模块获取量子密钥更新参数并发送报文，该报文经过量子加密，报文内容主要包含量子加密模块标识、密钥请求参数。报文到达量子密钥云平台侧进行解析，利用一级量子密钥加密更新的二级量子密钥构造响应报文返回终端或平台，终端或平台再与量子加密模块交互完成量子密钥更新。量子密钥分发更新报文扩展如表2所示。终端或后端平台到量子密钥云平台的量子密钥更新请求报文，报文类型为0x0090。

表2　量子密钥分发更新报文扩展表

起始标识 2字节	报文长度 2字节	报文类型 2字节	封装数据域 量子密钥更新数据	校验和
EAE0				

量子密钥分发请求报文如表3所示，报文示例：EAE0 NN 0090 0C9378651257D8A7 SSSS CS（报文总长度不超过2 K）。

表3　量子密钥分发请求报文

起始 标识 2字节	报文 长度 2字节	报文 类型 2字节	封装数据域 量子密钥更新数据 量子加密模块标识 （8字节）	封装数据域 量子密钥更新数据 密钥更新 请求	校验 和
EAE0	NN	0x0090	0C9378651257D8A7	SSSS	

量子密钥云平台到终端的量子密钥更新报文如表4所示，应用类型为0x0091，报文示例：EAE0 MM 0091 0C9378651257D8A7 DDDD CS（报文总长度不超过2 K）。

表4　量子密钥分发更新报文

起始 标识 2字节	报文 长度 2字节	报文 类型 2字节	封装数据域 量子密钥更新数据 量子加密模块标识 （8字节）	封装数据域 量子密钥更新数据 密钥更新 响应	校验 和
EAE0	MM	0x0091	0C9378651257D8A7	DDDD	

3 面向5G网络的量子加密应用

3.1 视频会议量子加密应用

视频会议系统是智慧城市各行业信息化建设的一部分，视频通信具备及时性、可靠性、灵活性等特点，可以应用于日常办公协作、培训、会议、统一调度等工作沟通中，实现总部与分部之间的互联互通。政府、金融、能源等行业的音视频数据重要程度较高，但一般的数据传输链路尚未进行有效的保护，存在一定的风险，迫切需要解决音视频的传输安全问题。可以在视频会议系统的传输链路中运用量子通信加密技术，针对所有数据信息实现基于量子密钥的加密传输。

使用量子加密技术提供的量子加密保护可实现一话一密、一机一算法的高安全强度的即时通信功能。比如银行内部人员之间的企业秘密沟通，可以得到高可靠的安全保障，大客户可以通过远程非接触的方式联系银行工作人员，交代一些个人隐私信息，无需赶赴网点当面交代、办理。营业网点可及时接收到上级最新指令，进行业务推广及厅堂营销。同时，可以将量子通信技术融入到业务办理流程中，保证远程视频柜员机（VTM）等智能设备的业务交互安全。基于量子加密技术的视频会议整体架构如图5所示。

3.2 集群对讲量子加密应用

根据业务实际需求，将集群对讲平台与量子加密技术融合，进行技术创新和应用实践的探索，可对各

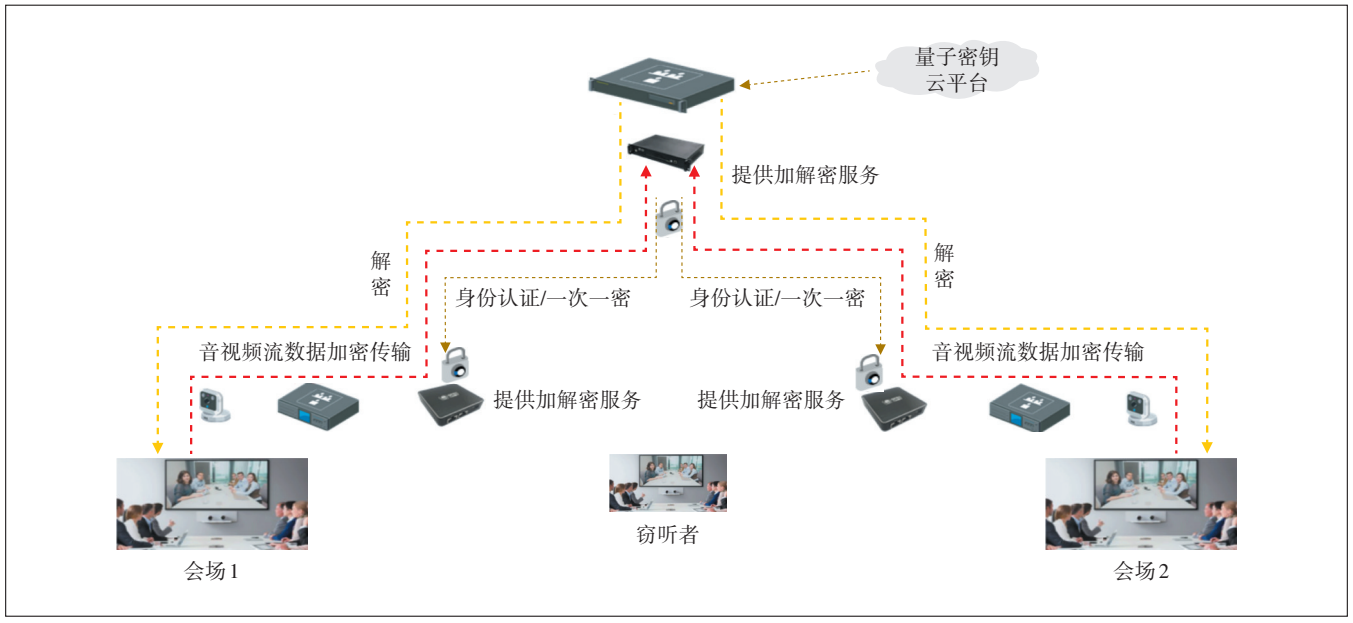

图5　基于量子加密技术的视频会议整体架构

类客户的企业管理、辅助决策提供必要技术支撑，实现5G无线网络集群对讲的安全通信和业务应用，确保稳定性、可靠性、高效性。集群对讲平台的对讲终端配合量子密钥云平台，通过量子加密实现终端的语音加密、视频加密、短信加密等。量子加密技术的应用，将全面整合信息资源，进一步提升工作效率，增强业务通信安全保障。基于量子加密技术的集群对讲整体架构如图6所示。

3.3 无人机量子加密应用

基于5G网络的电力无人机巡检应用场景构建量

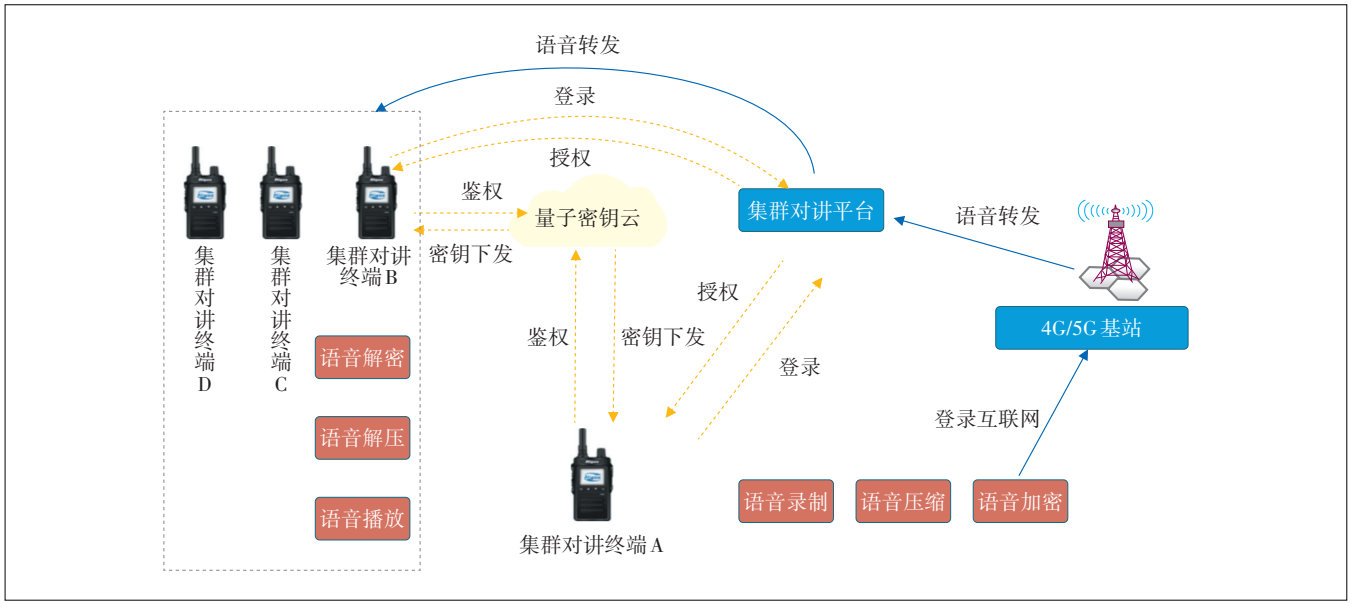

图6　基于量子加密技术的集群对讲整体架构

子密钥云平台，管控量子密钥从产生、分配、分发到使用、销毁等整个生命周期的相关功能。量子密钥云平台能够从量子随机数发生器获取量子密钥，安全存储、管理并分配这些量子密钥。同时，通过安全的密钥分发机制把量子密钥分发到使用端，满足端到端抗量子计算攻击的安全传输能力。基于量子加密技术

的无人机整体架构如图7所示。

4 总结

在智慧城市中，5G网络将作为基础网络实现万物互联，各种智慧城市的应用都将建设在5G网络上。本文提出的面向5G无线网络分发量子随机数的应用，意味着量子加密技术可与各种基于5G网络的智慧城市业务相融合，为数据传输安全成本巨大的传统问题提供一种可行的解决思路，有助于解决传统安全问题，达到提升终端信息安全保障性能、提升终端远程控制安全水平和业务安全保障水平的目标，更好助力智慧城市的未来发展。

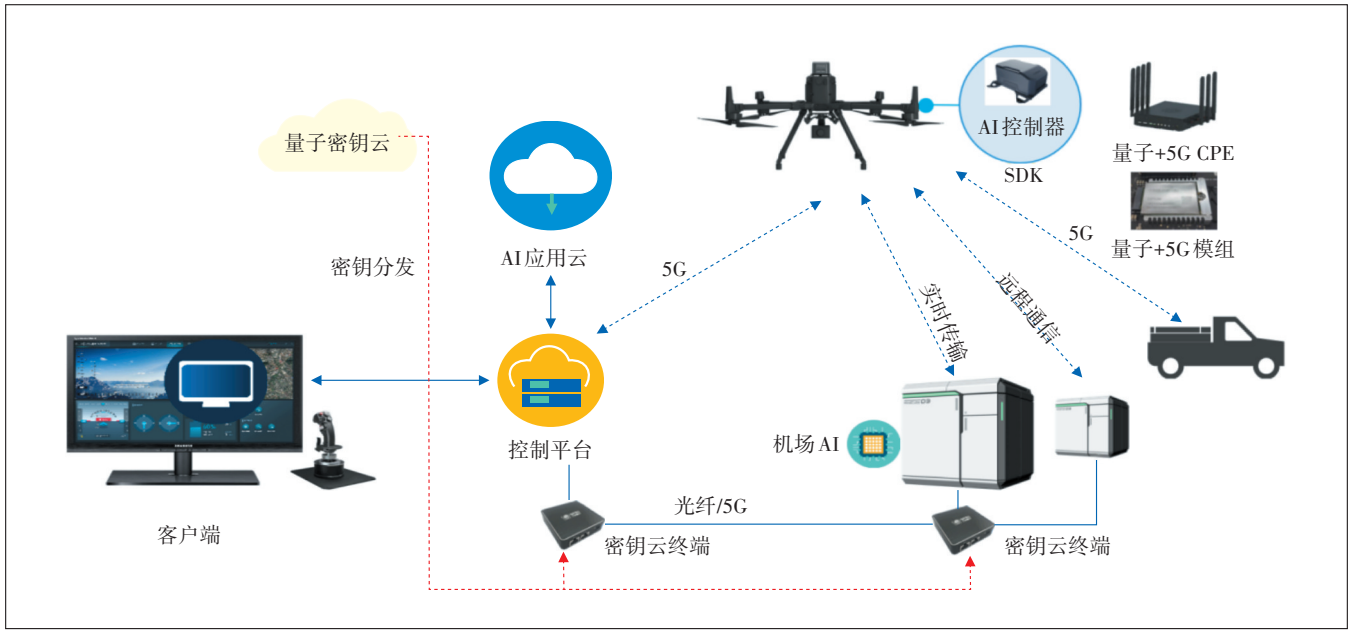

图7　基于量子加密技术的无人机整体架构

参考文献：

[1] EL-LATIF A A A, ABD-EL-ATTY B, MAZURCZYK W, et al. Secure data encryption based on quantum walks for 5G Internet of things scenario[J]. IEEE Transactions on Network and Service Management, 2020, 17(1): 118-131.

[2] 阳陈锦剑，余晓光，余滢鑫，等. 5G无线接入网安全研究[J]. 信息安全研究，2021，7(5)：457-465.

[3] 邱勤，张峰，何明，等. 5G行业专网安全技术研究与应用[J]. 保密科学技术，2021(4)：41-46.

[4] 郑东，张应辉. 密码技术在5G安全中的应用[J]. 信息安全与通信保密，2019(1)：50-58.

[5] 陈杰. 量子通信及其在电力通信中的应用分析[J]. 无线互联科技，2018，15(14)：10-11.

[6] 李孜峰，黄少华. 5G网络无线接入安全技术的研究[J]. 电子世界，2021(19)：182-183.

[7] 郭光灿. 量子信息技术研究现状与未来[J]. 中国科学(信息科学)，2020，50(9)：1395-1406.

[8] BORODIN M, ZHILYAEV A, URIVSKIY A. Key generation schemes for channel authentication in quantum key distribution protocol[J]. IET Quantum Communication, 2021, 2(3): 90-97.

[9] KAKKAR A. A survey on secure communication techniques for 5G wireless heterogeneous networks[J]. Information Fusion, 2020, 62: 89-109.

[10] ZHUANG L, HU J, CHENG J. Multilayer WFRFT and chaotic encryption wireless communication system based on MIMO[J]. Journal of Physics-Conference Series, 2020, 1453: 012116.

[11] 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.

[12] 赖俊森，赵文玉，张海懿. 量子保密通信技术进展及应用趋势分析[J]. 信息通信技术与政策，2020(12)：64-69.

[13] 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.

作者简介：

杜忠岩，毕业于华中科技大学，高级工程师，硕士，主要从事移动通信、智慧城市等技术研究工作；冷超，毕业于南京邮电大学，工程师，主要从事量子通信、智慧交通等技术研究工作；王题，毕业于华中科技大学，教授级高级工程师，双学位学士，主要从事移动通信、大数据、智慧城市等技术研究工作；黄大骏，毕业于中国科学技术大学，高级工程师，博士，主要从事量子通信技术和高速电子学研究工作。