量子保密通信技术及其在智慧城市中的应用研究

Research on Quantum Secure Communication Technology and Its Application in Smart City

冷　超[1]，杜忠岩[1]，王　题[1]，方分分[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）

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

摘　要：

随着数字经济发展步伐加快，网络安全、数据安全问题变得更加重要，随时可能影响智慧城市发展，甚至危害社会安全和国家安全。QKD基于量子力学基本特性，能够提供无条件的安全性保证，与经典数据传输网络融合，解决量子保密通信和经典通信协同应用问题。研究了QKD应用的基础原理、关键技术和网络架构，探讨融合方法和创新应用方案，实现智慧城市更安全可靠的数据加密传输。

关键词：

量子保密通信；量子密钥分发；数据传输网络；量子安全

doi：10.12045/j.issn.1007-3043.2023.04.008

文章编号：1007-3043（2023）04-0033-05

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：

With the acceleration of the development of digital economy, network security and data security issues become more important, which may affect the development of smart cities at any time, or even endanger social security and national security. Based on the basic features of quantum mechanics, QKD can provide unconditional security guarantee, integrate with classical data transmission network and solve the problem of quantum secret communication and classical collaborative communication application. It researches the basic principle, key technology and the network architecture of QKD application, discusses the application of fusion method and innovative application scheme, achieves more secure and reliable data encryption transmission for smart city.

Keywords：

QSC; QKD; Data transmission network; Quantum security

引用格式：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.

0 前言

智慧城市的建设是以信息化为支撑的，随着大数据的快速发展，信息安全需求越来越突出，如何应对智慧城市信息安全问题已成为下一代信息通信系统必须考虑的问题。基于量子物理基本原理的量子密钥分发（QKD）技术提供了不再依赖数学计算复杂度的新型密钥分发方法。通过这种具有信息理论安全特性的密钥分发方式，即使通过不安全的信道分发密钥也可以保证安全，进一步结合OTP方案或其他加密算法后可以有效地提高智慧城市信息安全性，抵御量子计算带来的安全威胁。

将QKD与经典密码学技术结合，打造基于量子保密通信技术的智慧城市安全防护体系，解决量子保密通信和经典通信协同应用问题，促进量子保密通信技术在智慧城市的推广应用。

1 智慧城市信息安全的需求分析

1.1 现状分析

1.1.1 量子安全竞争激烈

世界各国，特别是科技强国都想赢得“量子霸权”，并从国家层面提出了量子战略和量子项目，促进量子科技发展。比如美国，计划于5年内，在人工智

基金项目：国家重点研发计划（2019YFB2103200）

收稿日期：2023-02-28

能、量子通信等十大关键领域陆续投入1 100亿美元，大力支持这些领域的基础性与先进性技术研究、商业转化和教育培训等。

1.1.2 智慧城市应用加密强度不够

随着智慧城市应用规模的不断扩大，各项业务系统的运行与控制越来越依赖信息交互式的通信传输，其安全防护需求更加复杂。一方面，中间人欺骗、网络嗅探分析、数据爆破等攻击方式严重挑战现有的智慧城市安全防护手段；另一方面，智慧城市基础设施暴露在公共环境或使用公网通信设备时，存在被黑客入侵破解的安全隐患。需要深入研究智慧城市安全防护措施，提升信息安全防护体系。

1.1.3 量子计算机的算力挑战

量子计算机具有强大的并行运算能力，它能快速完成经典计算机无法完成的任务，这种优势在加密和破译等领域有着巨大的应用价值。在量子计算机出现以后，智慧城市应用基于数学理论的密码体系将不再安全，该体系能够被量子计算机快速破解，研制可以抵抗量子计算攻击的方法已经成为当务之急。

1.2 发展需求

1.2.1 国家层面的支持

2020年10月16日，中共中央政治局就量子科技研究和应用前景举行第二十四次集体学习。习近平总书记强调，量子科技将引领新一轮科技革命和产业变革方向，要充分认识推动量子科技发展的重要性和紧迫性，并要求找准我国量子科技发展的切入点和突破口，培育量子通信等战略性新兴产业。国家“十四五”规划将“量子信息”列为“十四五”重点突围的核心技术，指出要加快布局量子计算、量子通信等前沿技术。

1.2.2 网络安全的需要

当前智慧城市应用场景面临的网络恶意攻击、数据窃取、病毒、勒索等事件呈上升态势，各行业也更加重视网络安全，紧密跟进安全技术的发展，探索全面保障数据安全的产品，加强全方位网络安全管理。

1.2.3 数据安全的需要

信息技术的快速发展，特别是智慧城市新型应用正在快速落地，智慧城市物联网正被广泛应用，对网络安全行业提出了更高的要求，信息安全产业面对着巨大的安全压力，同时也拥有巨大的发展空间。

量子通信技术可以为智慧城市新型应用的数据传输提供安全可靠的加密保护。通过一次一密的加密手段，任意双方可以实现无条件安全的加密通信，也支持按需更换密钥，提升智慧城市新型应用安全防护水平。

2 整体架构与关键技术

2.1 QKD与经典网络融合整体架构

基本的QKD量子保密通信系统由一对通过量子信道连接的设备组成，可以实现点对点链路上信息理论安全的对称密钥分发，能够不受窃听攻击的影响。同时，QKD使用国密算法加密，与经典数据传输网络深度融合，将成为下一代数据通信的研究重点。

在智慧城市应用中，量子密钥分发QKD网络与经典数据传输网络融合时，QKD的使用如图1所示。信息发送方Alice的QKD产生完全随机的量子态，并通过量子信道发送给接收方Bob的QKD。在双方都收到原钥后，QKD先进行信息比对确认传输通道没有被窃听，并通过基矢比对筛选密钥，然后进行相应的纠错和保密增强处理，形成最终的密钥。这些被确认安全的密钥由QKM进行储存和管理。当经典信道业务数据需要密钥进行加密传输时，将密钥从QKM中调用出来进行数据加密。通过这种方式，整个系统实现了无条件安全的保密信息传输。

在实际建设中，要尽可能不影响已有网络拓扑结构和已有业务系统的正常运行，通常采用的建设方法如下。

a）不改变现有数据传输网络结构，增加QKD量子保密通信系统，对现网设备进行数据级的安全加密。

b）建立数据加密体系，对基站设备、光传输节点、核心交换设备、后台管理中心之间传输的业务数据进行加密，防止恶意窃听、篡改和伪造。

c）建立终端准入机制，识别接入终端，具备黑白名单功能，禁止非法终端接入。

d）搭建网络系统监测平台，收集监测生产网网络与系统运行状态，及时发现异常情况和恶意入侵行为。

将QKD技术协商的密钥应用于经典数据传输网络中的身份认证和会话协商，保障智慧城市应用数据的安全、可靠传输，覆盖数据的全生命周期。

2.2 共纤融合传输技术

共纤融合传输技术可以将量子密钥分发设备所发出的量子光信号、同步光信号以及用于协商的正反向经典光信号通过波分复用技术进行融合传输，将原

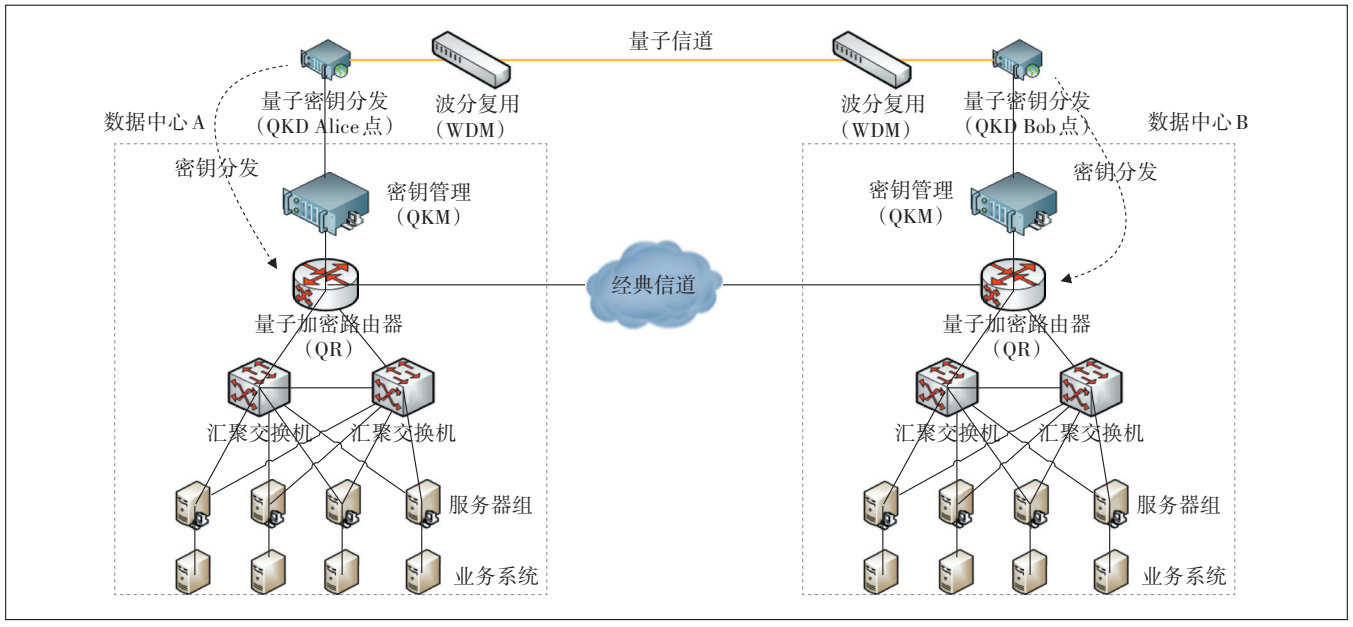

图1　QKD与经典数据传输网络融合架构

本在多根光纤中传输的信号合并到一根光纤中，可有效节省量子保密通信网络部署所需的纤芯资源，实现经济、高效建网的目标。

该技术需要调节经典光信号与同步光信号的光强，降低对量子光信号的影响，主要需要解决功率较强的经典通信中光信号的功率谱噪声和拉曼散射、四波混频等非线性噪声对量子通信的干扰问题。

2.3 密钥产生及应用流程

从密钥的产生及应用角度分析，可以分为密钥产生层、密钥管理层和密钥应用层，其具体流程及数据传输关系如图2所示。

2.3.1 密钥产生层

密钥产生层的核心技术是QKD，负责产生原始密钥。具体过程是由QKD-Alice端制备量子态信号并通过激光器发送到QKD-Bob端，QKD-Bob端采用单光子探测器接收量子态信号，从而完成原始密钥的收发。该原始密钥不能直接使用，需要经过基矢比对、纠错、保密增强成为量子密钥。

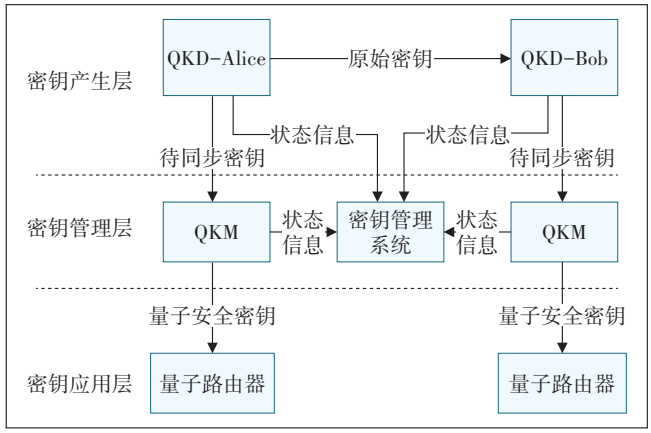

图2　流程及数据传输关系

2.3.2 密钥管理层

密钥管理层主要包含QKM及密钥管理系统，该系统负责密钥的提取、同步、存储和服务，实现对量子网络设备的统一管理。密钥管理层管理整个QKD网络，并向密钥应用层提供量子安全密钥，是量子密钥分发体系的安全核心，实现身份认证、权限管理等功能。

2.3.3 密钥应用层

密钥应用层是一个开放的体系，支持多种安全设备接入，如量子加密路由器、加密机、密钥云系统等。量子加密路由器从密钥管理系统中请求量子安全密钥，用于本地的数据加密业务。

2.4 量子密钥分发技术

QKD以量子态为信息载体进行远程密钥分发，基于量子物理原理能够实现抗截获、抗破译和窃听可感知，为双方提供安全的密钥分发机制，从而从整体上提升智慧城市应用中密钥管理的安全性与独立性。基于诱骗态BB84协议的QKD设备系统主要包括设备初始化、量子态制备、测量、基矢比对、纠错和保密增强等过程。

2.5 量子加密路由技术

量子加密路由技术是结合量子加密技术和对称式加密技术的新一代高保密量子安全加密技术，可对接量子真随机数发生器或量子密钥分发设备，开辟IPSec VPN加密通道后可调用量子真随机数发生器或者量子密钥分发设备协商出来的随机数，将随机数作为协商会话密钥，运用对称加密密钥和国密算法对数据通信链路中的数据进行加密后密文传输。该技术为数据传输提供完整性验证、数据源认证、抗重播等安全传输服务，确保黑客无法运用侦听程序截获或破解数据信息，保障数据的安全性、可靠性。

3 典型应用场景

基于QKD的量子保密通信作为量子通信现阶段发展相对成熟并具备产业化潜力的代表性技术，有望成为面向量子时代的重要密码学组件，和经典数据传输网络深度融合，为智慧城市数据传输提供全新的安全解决方案，赋能各行业智慧发展，应用价值和前景非常广阔。

3.1 智慧城市数字政府量子安全组网

智慧城市数字政府量子安全架构如图3所示。在新型智慧城市和数字政府的建设中，可依托QKD和经典数据传输网络深度融合的量子保密通信系统，主动获取或自动接收A点或B点自动产生的量子密钥，并经过量子加密路由器传输至各应用系统或网络安全设备，提供加密所需的密钥源。

各类智能终端、应用系统、数据链路采用量子密钥进行整体加密，可安全、稳定运行在电子政务外网链路，为数字政府、数字化改革提供量子保密通信技术支撑，保障网络安全，推动数字政府密码基础设施建设。未来量子加密的数据传输网将成为政务网的发展趋势。

3.2 智慧城市数字电网量子安全组网

随着智慧城市数字经济发展，新型电网数字化建设逐步推进，网信安全也面临更大的挑战。依托量子保密通信系统可以实现按需更换密钥，保障电力主网与调度、配电主网等系统之间的数据安全。量子安全组网确保电网通信链路的数据安全，防止信息泄露、窃取、篡改毁损和丢失，保障电力应用安全稳定运行。智慧城市数字电网量子安全组网架构如图4所示。

3.3 智慧城市数字民生量子安全组网

在智慧城市数字民生的医疗业务场景中，随着电子医保、移动医疗等医疗信息化的普及，存在着医疗数据泄露的巨大隐患，所以加强医疗数据安全管控和个人隐私保护，提升医疗数据安全信息技术刻不容缓。可在医院信息集成平台和终端之间增加量子保密通信系统，实现量子加密传输，提高医疗业务数据

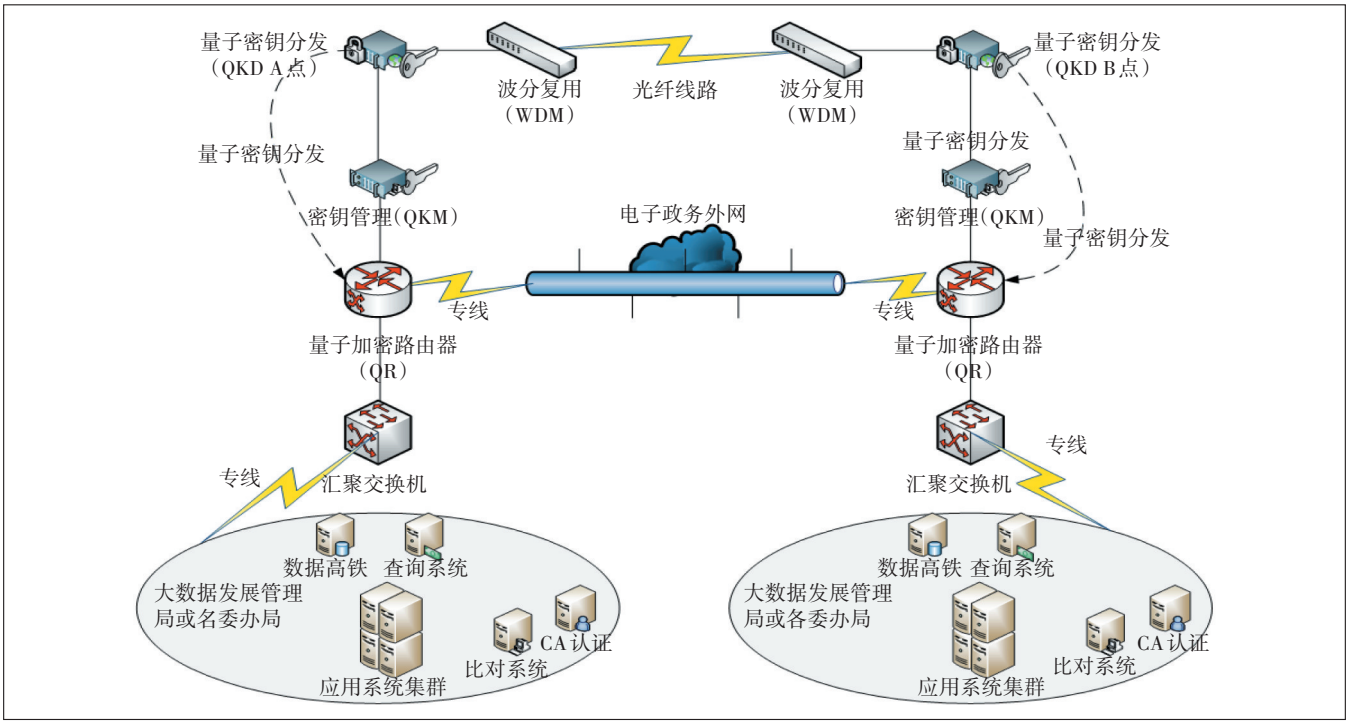

图3　智慧城市数字政府量子安全架构

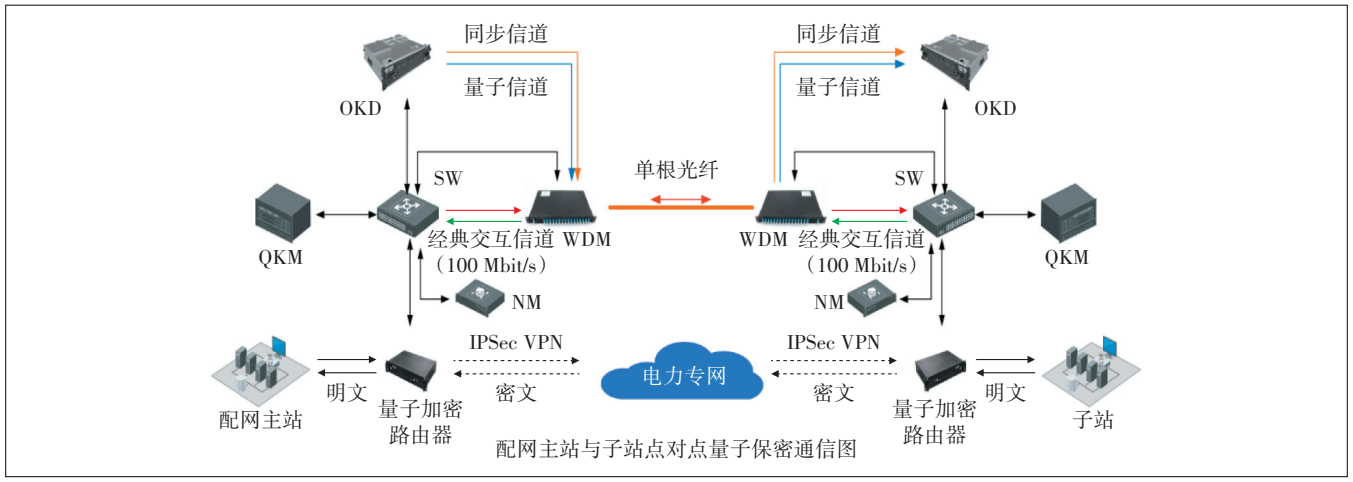

图4　智慧城市数字电网量子安全组网架构

传输的安全性，为业务应用提供从物理环节到网络通信、应用数据的全流程安全，助力构建数字民生的医疗安全防护体系。智慧城市数字民生量子安全组网架构如图5所示。

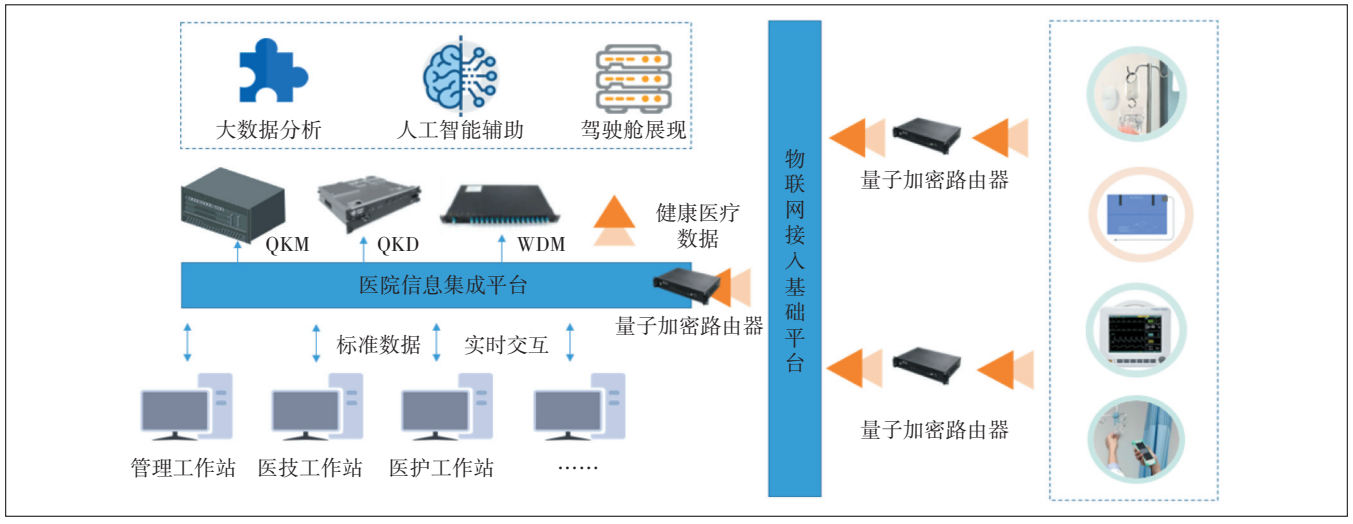

图5　智慧城市数字民生量子安全组网架构

4 结束语

量子通信是国家战略发展的前沿科技，将成为保障智慧城市应用安全的重要技术手段，也是当前理论和应用研究的热点。本文研究了QKD和经典数据传输通信网络的融合，构建量子密码分发和量子安全组网的架构体系，全面适用于政企数字化转型、数字化改革在信息化建设方面的高安全需求，更好地促进智慧城市行业应用。

参考文献：

[1] WU X D, WANG Y J, HUANG D, et al. Multi-mode plug-and-play dual-phase-modulated continuous-variable quantum key distribution [J]. Quantum Information Processing, 2021, 20(4): 143.

[2] 黄显明. 真随机数发生器在信息安全系统中的应用[J]. 电子产品世界, 2015, 22(6): 13-15.

[3] 栾欣，郭义喜，苏锦海. QKD网络中组密钥协商的研究[J]. 计算机应用与软件, 2015, 32(5): 267-269, 301.

作者简介：

冷超，毕业于南京邮电大学，工程师，学士，主要从事量子通信、智慧交通等技术研究工作；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；王题，毕业于华中科技大学，教授级高级工程师，双学士，主要从事移动通信、大数据、智慧城市等技术研究工作；方分分，毕业于杭州电子科技大学，高级项目经理，学士，主要从事数据通信和量子通信技术研究工作。