实用化光纤量子加密电话网络和高速数据传输系统 —— 现场应用与安全管理

吴华^{①†}, 赵于康^{②†}, 赵勇^{②③④}, 赵梅生^{④*}

① 中国科学技术大学公共事务学院, 合肥 230026

② 中国科学技术大学合肥微尺度物质科学国家实验室, 合肥 230026

③ 中国科学院量子技术与应用研究中心, 济南 250101

④ 山东量子科学技术研究院有限公司, 济南 250101

* 通信作者. E-mail: meisheng.zhao@quantum-info.com

† 同等贡献

收稿日期: 2013-09-17; 接受日期: 2014-02-19

山东省自主创新专项 (批准号: 2012CX30401) 资助项目

摘要 本文以如何应用量子通信技术满足现场应用和安全管理需求为出发点, 以国内最近完成的一个在现场光纤网络上搭建的多节点量子加密电话网络和高速数据传输系统为实例, 具体分析了为满足现场应用和安全管理的需求, 实用化光纤量子通信系统所采用设计方案, 并简单介绍了该系统实施和长期运行情况. 该系统满足了重要事务对于不同应用形式及高安全等级通信的需求, 并验证了实际应用环境下的可靠性和易用性, 具有很好的代表性. 本文也对量子通信系统应用于公共管理提出了建议.

关键词 量子通信 量子加密 网络分层 网络管理 数据安全

1 引言

现代公共管理的核心内容之一是借助网络信息技术的驱动实现更符合应用需求、更经济高效、更一体化的公共事务管理, 实现管理理念、管理体系的革新^[1]. 然而目前的网络信息技术还不能完全满足管理的需求, 特别是安全性问题一直缺乏有效的解决方法. 以近期“棱镜门”事件为代表的一系列安全性事件凸显了网络安全问题的广泛存在, 因为网络安全问题造成的损失正呈现上升趋势, 现有互联网的体系结构依靠打补丁的方式却无法遏制这种趋势.

量子通信是目前公认的唯一无条件安全的通信手段^[2~4], 有望从根本上解决通信安全这一经典网络核心难题. 目前, 光纤量子通信技术进入了实用化阶段, 已经可以有限规模地应用于网络化通信. 这样一种新兴的高安全通信技术, 必将对公共管理的应用形态和体系产生影响. 因此, 如何将量子通信技术用于公共管理, 满足相关的应用和管理需求成为现阶段的重要研究课题之一, 急需展开研究和试验.

量子通信应用包含多个环节, 无条件安全的量子密钥分发 (QKD) 是其核心支撑环节, 若需满足各类应用需求, 还需要 QKD 环节之后辅以相应的解决方案, 安全管理在保障其系统安全性方面同样具

引用格式: 吴华, 赵于康, 赵勇, 等. 实用化光纤量子加密电话网络和高速数据传输系统 —— 现场应用与安全管理. 中国科学: 信息科学, 2014, 44: 312-321, doi: 10.1360/N112013-00168

图 1 电话网络拓扑图

Figure 1 Topology of the telephone network

有重要的作用. 因此, 量子通信技术应用用于公共管理, 不仅必须符合应用的需求, 还需要融入先进的管理理念和管理体系. 从长远来看, 量子通信技术应用用于公共管理将会是一个相互渗透、共同发展的过程, 将会有大量问题有待探索解决, 因此现阶段不可能实现一步到位. 这也要求量子通信系统的设计必须具有足够的可塑性和兼容性, 并有序地进行探索试验.

近十年来, 国内外已建成不少基于现场光纤的 QKD 试验网络^[5~14]. QKD 技术的成熟也推动了产业的形成, 近年来在欧洲已经实现了不少商业化应用, 量子通信技术的标准化工作也取得了初步成果. 我国的 QKD 整体技术水平处于国际前列, 目前已完成一系列真实环境中的应用示范, 对符合应用需求的技术规范的研究和试验已初步展开.

最近我国又完成了一次重要的量子通信应用 —— 于 2012 年底在现场光纤上成功搭建了多节点量子加密电话网络和一套高速数据传输系统. 该系统一直稳定运行至今, 既满足了相关用户的实际应用需求, 同时也检验了系统整体的可靠性和易用性. 本文以此应用为实例, 对实用化量子通信系统如何满足安全管理和现场应用需求进行介绍和分析. 后文结构如下: 在第 2 节详细说明了为满足安全管理和现场应用的需求量子通信系统所采用的设计方案, 在第 3 节简单介绍了系统的实施和运行情况, 最后对本次应用试验进行了总结, 并对量子通信应用于公共管理的未来研究内容提出了建议.

2 量子加密电话网和高速数据传输系统设计

2.1 系统概述

整个现场系统包含量子加密电话网和高速数据传输系统两个互相独立的系统. 量子加密电话网支持多个用户进行一次一密的加密语音通信, 具有网络化应用形式和最高安全等级需求. 其拓扑如图 1 所示, 网络有 4 个终端节点和 1 个交换节点, 各终端节点均有光纤链路连接交换节点. 量子加密高速数据传输系统支持两地之间进行大量数据的高速传输, 具有干线应用形式和较高安全等级需求, 拓扑为点对点结构, 有一条单独的光纤链路.

图 2 系统分层模型

Figure 2 Layered system model

2.2 系统分层设计: 安全性、可塑性和兼容性

量子通信应用于公共管理, 在加强通信安全的同时还必须符合现场应用的需求, 并支持先进的管理理念和管理体系. 这个领域的研究还只是起步阶段, 还有大量的内容有待探索. 因此, 现阶段量子通信系统必须联合应用和管理其他环节共同实现目标, 一方面要确保量子通信系统本身的安全性, 另一方面在设计上应当具有足够的可塑性和兼容性, 既有足够的功能以支持多样的安全管理, 又能够尽量不限制其他环节的运行. 本系统遵从该原则进行设计开发.

在经典通信网络中, 早期为了降低开发和管理难度提出了分层设计的理念, 整个网络划分成物理层、数据链路层、网络层、传输层、应用层等具有相对独立逻辑功能的分层^[15]. 随着技术成熟度的提高和需求的提升, 特别是安全性需求的提升, 经典网络出现了分层扁平化的趋势. 原先的一些分层紧密联合成一个功能更丰富、效率更高的分层, 以支持安全性、智能化管理方面的需求.

参考经典网络的设计, 本文在量子通信系统结构设计时综合考虑了现阶段技术条件和现场应用、安全管理的需求, 采用了 QKD 层、密钥管理层、应用层的分层设计, 如图 2 所示. 三层结构的设计为近期的量子通信网络普遍采用, SECOQC 网络^[6]、SwissQuantum 网络^[9]和东京 QKD 网络^[13]就采用该模型. 出于对安全性和系统本身管控的考虑, 本系统在具体的设计上有很大的不同. 设计了用量子密钥对设备认证、控制指令、业务数据等多个环节进行贴身保护, 管控功能更丰富的扁平化密钥管理层; 并保留了应用层的相对独立性, 以满足用户对于应用多元化、灵活性以及沿用原有管理体系等方面的需求.

密钥管理层由量子密钥生成控制系统和密钥管理系统组成, 其中量子密钥生成控制系统用于控制多个终端节点进行分时的互联, 该功能由单独的服务器实现. 而密钥管理由 QKD 终端集成的功能模块实现, 其核心是载入了自定义管理策略和隔离策略的 FPGA. 密钥管理层集成了密钥生成控制、密钥管理等多项功能, 并嵌入加解密功能. 同时, 相应地在应用层和 QKD 层增加了管控接口. 为了提高系统的安全性, 密钥管理和高安全等级的业务加解密 (一次一密) 由一个 FPGA 完成, 实现加密功能的同时确保量子密钥不需要在不同分层设备间转移. 实际上, 本文对密钥管理层的这种强化设计还能

支持密钥中继路由控制和核心设备控制指令保护. 与本文设计不同, 在其他量子网络中加解密和密钥管理相对独立, 保护范围一般仅限于业务数据.

在本系统中, 应用层主要包括常规的应用终端、业务综合接入系统和信令系统. 在强调多环节贴身保护的同时, 通过业务综合接入系统尽可能地保留了上层应用形式的独立性, 常规设备接入即可使用并基本保留原有功能和使用形式, 从而保障了上层应用形式的丰富性和灵活性, 并且支持用户使用常规的管理体系. 另外, 针对高速数据传输系统的高吞吐量需求和点对点通信的简单结构, 其应用层额外部署了一个加解密引擎.

QKD 层则包括 QKD 模块和量子网络组网设备, 如: 光交换机.

2.3 QKD 层: 无条件安全的核心支撑

QKD 层部署了山东量子科学技术研究院生产的 QGW 01AB20-II 型量子网关, 该量子网关集成诱骗态方案光源、四通道近红外单光子探测器和双向 QKD 模块, 能够实现收发一体的 QKD. 其中 QKD 使用 BB84 协议^[16]和诱骗态方案^[17~19], 并采用偏振编码方案. BB84 协议和诱骗态方案是安全性研究最透彻的协议和方案, 其无条件安全性由物理原理保障并完成了理论证明^[2~4], 为大多数 QKD 系统所采用. 偏振编码方案更适合组建动态互联网络, 并且使用该方案的单发射终端可以做到十分便携, 是目前主流的编码方案. 通过偏振反馈补偿, 偏振编码方案受信道影响较大的缺点目前已经能够有效抑制^[14].

QKD 层的安全性是量子通信的核心要素, 必须采取一系列措施来消除非理想条件形成的安全隐患, 下面就这些措施进行具体说明.

在 QKD 协议实现的安全性方面, 由于环境噪声、系统错误或者人为攻击等各种因素, 经过基矢比对得到的初始量子密钥不可避免的存在一定的错误率, 容忍这些错误则可能被攻击者掌握部分信息. 因此, 需要从初始量子密钥中提炼安全的密钥. 安全密钥提炼包含纠错和隐私放大两个步骤, 所提炼密钥的安全性由信息论相关理论保障. QGW 01AB20-II 型量子网关采用 CASCADE 算法^[20]完成纠错, 并使用 Toeplitz 随机矩阵实现的 Universal-2 类的 Hash 函数^[21]进行隐私放大.

在 QKD 设备合法性方面, 消息认证是防止中间人攻击的唯一方法. QGW 01AB20-II 型量子网关采用 Wegman-Carter 认证方案^[22,23]. 该认证方案需要 Universal-2 类的 Hash 函数族, 该 Hash 函数族的实现方法也源自文献^[21]. 消息认证的初始密钥通过预置方式分配, 一旦 QKD 过程完成后, 认证密钥则取自量子密钥. Wegman-Carter 认证方案是一种单次使用的无条件安全认证方案, 每次认证都需要更换一段密钥. 因此, 量子网关对认证设置了超时限制, 认证失败次数超过限制时, 会停止认证过程并发出警报.

在 QKD 设备的器件非理想性方面, 已知的漏洞已全部消除. 近年来出现的强光致盲攻击^[24]是一种利用器件弱点攻击 QKD 系统的量子黑客攻击方案, 因为在原则上可完全窃取量子密钥而备受关注. QGW 01AB20-II 型量子网关在这方面采取了充分的防护措施, 其探测器具有强光报警功能, 当强光侵入系统造成探测器工作状态不正常时, 探测器会向系统报警.

2.4 密钥管理层: 智能的安全管理功能

密钥管理包括密钥的生成、使用和销毁, 由于关系到量子密钥的安全性, 所有环节都必须进行安全管理. 特别要指出的是, 这些管理技术和经典网络安全管理的相关技术是通用的.

在本系统中, 量子密钥由 QKD 过程产生, 而 QKD 的触发和关闭由密钥生成控制系统完成. 电话网络和高速数据传输系统都采用了软件实现密钥生成控制. 这是因为和经典密钥管理中的生成不同, 这里的密钥生成控制系统不涉及密钥内容, 其安全漏洞不会降低安全性, 只对系统的鲁棒性有影响.

密钥的使用和销毁主要由密钥管理系统完成. 我们先比较一下密钥管理功能的实现方式及其关键特点. 在目前已知的欧美的试验网和应用实施中, 密钥管理多由软件实现. 软件实现的优势是灵活, 主要的缺点是安全性依赖于操作系统和操作规范的管理. 根据目前的经验, 采用 linux 操作系统, 关闭多余的网络端口并进行适当的内核裁剪, 能够较大程度保障操作系统的安全. 但是面对层出不穷的黑客技术, 需要及时升级系统并评估系统后门对密钥存储安全性的影响. 硬件实现密钥管理则相反, 缺点是不够灵活, 不能快速地进行多种管理策略的配置, 优点是功能固化后具有很高的安全性, 并且操作规范管理方面的要求极大降低. 在本系统中, 密钥管理使用了软、硬件结合的实现方式, 其中量子加密电话网使用硬件实现密钥管理, 量子加密高速数据传输系统采用软、硬件联合实现密钥管理.

本系统中密钥管理系统的基本功能包括密钥获取、密钥使用管理、逻辑隔离、加解密或者密钥导出、密钥废弃. 下面基于密钥管理的硬件实现方式对各项基本功能进行具体说明.

1) 密钥获取. 将 QKD 系统通过串行方式输入到系统的密钥数据进行串并转换, 使串行数据变为密钥管理所需的并行数据格式, 密钥获取在 FPGA 中完成.

2) 密钥使用管理. 密钥使用管理的具体功能包括密钥存储、密钥读取、密钥状态上报、密钥同步、密钥校验等. 其中密钥存储、密钥读取和状态上报由 FPGA 本地完成, 密钥同步和密钥校验功能都需按照自定义协议, 在两个密钥管理系统间协商完成.

3) 逻辑隔离. 确保量子密钥不会被公网接触到, 同时实现对公网接收到的数据进行判断, 仅让合法的数据进入到后续模块. 逻辑隔离通过 FPGA 实现, 任务包括数据帧的解析、数据帧的过滤、加解密密钥的读取、数据帧的加解密、数据帧的组装, 同时 FPGA 在固化的功能中无条件禁止密钥输出.

4) 加解密或密钥导出. 在量子电话网中, 一次一密方式的加解密及其他密钥管理功能由同一个 FPGA 完成, 以确保最高等级的安全性. 在量子加密高速数据传输系统中, 由于加解密由单独的模块完成, 量子网关需要将密钥按照固定格式输出给其他应用层设备, 此时逻辑隔离需要联合上层模块来完成.

5) 密钥废弃. 根据使用策略对密钥进行操作屏蔽或擦除. 在“一次一密”加密方式下, 密钥存储池中使用过的密钥将不能再被读取, 并在一定周期后被覆写.

2.5 应用层: 灵活兼容应用、管理系统

量子加密电话网的应用层包括: 普通电话、内置于量子网关的综合接入系统、信令服务器. 综合接入系统可以对普通电话的信令信号进行解析, 将业务数据送往量子网关的密钥管理系统, 将信令路由至信令服务器处理, 从而保留拨号呼叫、建链、摘机振铃、挂机等电话呼叫流程. 通过综合接入系统的协议解析, 本文比较高效地实现了应用层的相对独立, 普通电话接入量子加密电话网即可使用, 同时大部分功能如一键拨号等均得到保留.

量子加密高速数据传输系统的应用层包含常规的业务服务器和信令系统, 并使用单独的加解密服务器实现对业务数据的处理. 使用单独的加解密服务器能够支持灵活的加解密策略, 同时可以灵活地捆绑到经典网络分层中. 其加密算法采用 AES-128 算法, 密钥由量子网关提供, 每组密钥加密 N 个数据包后即更换, N 的值可以在 1~10000 间任意设置, 加解密吞吐量达到 200 Mbps 以上. 另一方面, 该服务器工作于网关模式, 在 TCP 协议层实现业务数据加解密. 这种方式也保留了应用层的相对独立,

图 3 量子加密电话网设备连接图

Figure 3 Wiring diagram of the telephone network with quantum encryption

可用来实现其他任何基于 TCP/IP 协议的私有网络通信应用. 实际上, 利用量子加密高速数据传输系统, 本文还采用商用视频电话设备同时搭建了一套视频电话系统. 量子网关和解密服务器对于视频电话系统都是透明的, 用户使用体验完全等同于普通视频电话.

3 实施和运行情况

3.1 设备配置

量子加密电话网. 量子加密电话网的设备配置如图 3 所示. 量子网关通过全通型光量子交换机动态地实现各节点间的分时互联, 从而组成了一个分时全通的 QKD 网络. 同时还有一个经典的私有局域网用于业务数据、密钥管理和 QKD 协商交互数据的传输. 量子加密电话网使用了由山东量子科学技术研究院生产的 QGW 01AB20-II 型量子网关. 这是一个融合式设备, 集成了应用层的综合接入系统、密钥管理层和 QKD 层的各功能模块. 电话业务的信令服务器、量子密钥生成控制服务器都和经典交换机部署在一起, 均通过以太网口连接交换机. 光量子交换机也和交换机部署在一起, 通过以太网口连接网络, 接收量子密钥生成控制服务器的相关指令. 网络管理系统在图中没有画出, 前文也未提及. 实际上量子网关支持部分网络管理功能: 采用标准 SNMP 协议, 量子网关的状态信息可通过内部的网管代理端上报网管服务器; 同时原则上通过网管服务器可以远程管理设备状态, 不过考虑到系统的高安全性要求, 目前仅开放了重启等有限的管理功能. 由于量子加密电话网架设在用户单位的私有光网络上, 因此系统中并没有配置防火墙, 同时量子网关使用基于 FPGA 的硬件隔离提供了一部分防入侵功能. 原则上, 将电话网系统的用户端置于防火墙后工作并没有困难.

量子加密高速数据传输系统. 量子加密高速数据传输系统是一个点对点系统, 业务服务器是用户单位原有的数据库服务器. 和电话网相比, 该系统的主要差别是使用了单独的服务器以软件方式实现密钥管理和大吞吐量加解密. 该服务器操作系统为国产中标麒麟安全操作系统, 并关闭了不必要的

图 4 量子加密高速数据传输系统设备连接图

Figure 4 Wiring diagram of the high speed data transmission system with quantum encryption

表 1 线路光纤衰减值

Table 1 Loss value of installed fiber

Number	Link	Loss value (dB)
1	Telephone network node 1—Route node	-1.40
2	Telephone network node 2—Route node	-1.05
3	Telephone network node 3—Route node	-4.29
4	Telephone network node 4—Route node	-6.63
5	High speed data transmission system	-6.97

网络端口。出于同样的考虑, 量子加密高速数据传系统也没有配置防火墙, 但加入防火墙并没有原则性的困难。

3.2 线路整治与安装调试

在系统的实施过程中, 现场能使用的光纤较为老旧, 所有线路的衰减均远超过每公里 1 dB. 高速数据传输系统的光纤链路超过 15 km, 衰减超过了量子网关的工作范围. 针对这一问题, 本文选择了对原有线路进行整治优化的方案, 相比重新敷设线路方案可显著节约人财物时. 系统的安装调试简便, 均由设备供应商的技术人员完成. 运行期间, 系统维护由经简易培训后的用户单位工作人员负责, 不需要技术人员额外参与。

3.3 运行情况

现场光纤线路状况列表如表 1 所示, 其中高速数据传输系统链路的光纤衰减值为整治后数据. 从表中可见电话网节点 3 和节点 4 互联时, 链路衰减最大, 加上光交换机的衰减后达到了约 -12 dB. 其余节点互联时链路衰减均小于 9 dB. 实际运行中, 节点 3 和节点 4 间量子密钥成码率较低, 在此链路上拨打加密电话时需要使用存储密钥. 其余节点互联时量子密钥生成速率均在 5 kbps 以上, 可满足实时“一次一密”的双工语音电话加密需求。

电话网系统从2012年四季度开始投入使用后保持7×24小时运行,到目前为止已稳定运行近10个月. 高速数据传输系统与电话网同时投入使用,不同的是,该系统只在执行任务期间需要开机连续运行. 连续执行任务最长的时间也达到2周. 该系统主要负责加密传输异地数据库同步备份数据,执行任务期间,每次传输数据量达5 Gbyte以上. 系统表现了良好的可靠性,从未出现任何数据传输或者加解密错误.

各系统运行期间,负责维护的工作人员未发现任何死机或者其他影响系统功能与性能的重大异常现象. 技术人员事后检查系统日志,也证实在运行期间未发生任何重大故障.

4 总结与建议

本文以国内最近完成的一个重要应用——量子加密电话网和高速数据传输系统为实例,对量子通信系统如何满足现场应用和安全管理的问题进行了研究和试验. 系统采用QKD层、密钥管理层和应用层的三层结构设计,通过管控功能丰富、紧密结合加解密环节的密钥管理层实现了对量子通信系统本身的智能化安全管理,并能够支持最高安全等级的通信应用. 通过保留应用层独立性的设计满足了现场应用多元化、灵活性的需求,支持用户使用自有的通信设备和管理体系. 通过这种设计,系统同时兼顾了安全性、可塑性和兼容性. 系统在长期运行中用户体验良好,性能稳定,显示了系统设计的合理性,同时也表明国产QKD设备已具备了较好的成熟度和可靠性.

本次应用是我国在量子通信服务于现场应用和安全管理方面一次具有代表性的成功尝试. 在今后的研究中,如何使量子通信系统紧密、高效地融入现代公共管理体系,如何实现跨平台整合,如何在私有网架设向公网架设转移时进行更完善的管理比如操作人员管理,如何满足更多元化应用的需求,在新兴技术驱动下管理形态和体系将如何演进等问题将是值得关注的内容.

致谢 感谢安徽量子通信技术有限公司的许鹰工程师提供了实施经验和有益的建议.

参考文献

- 1 Cai L H. E-Government: Reengineering Government in Information Age. Beijing: China Social Science Press, 2006. 13–18 [蔡立辉. 电子政务: 信息时代的政府再造. 北京: 中国社会科学出版社, 2006. 13–18]
- 2 Lo H-K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 1999, 283: 2050–2056
- 3 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett*, 2000, 85: 441–444
- 4 Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices. *Quant Inf Comput*, 2004, 4: 325–360
- 5 Elliott C, Colvin A, Pearson D, et al. Current status of the DARPA quantum network. In: Donkor E J, Pirich A R, Brandt H E, eds. *Quantum Information and Computation III*. Bellingham: SPIE, 2005. 138–149
- 6 Peev M, Pacher C, Alléaume R, et al. The SECOQC quantum key distribution network in Vienna. *New J Phys*, 2009, 11: 075001
- 7 Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt Express*, 2009, 17: 6540–6549
- 8 Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network. *Opt Express*, 2010, 18: 27217–271225

- 9 Stuck D, Legré M, Buntschu F, et al. Long-term performance of the Swiss quantum key distribution network in a field environment. *New J Phys*, 2011, 13: 123001
- 10 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chin Sci Bull*, 2009, 54: 2991–2997
- 11 Chen W, Han Z F, Zhang T, et al. Field experiment on a star type metropolitan quantum key distribution network. *IEEE Photon Technol Lett*, 2009, 21: 575–577
- 12 Wang S, Chen W, Yin Z Q, et al. Field test of wavelength-saving quantum key distribution network. *Opt Lett*, 2010, 35: 2454–2456
- 13 Sasaki M, Fujiwara M, Ishizuka H, et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt Express*, 2011, 19: 10387–10409
- 14 Lanco D, Martinez J, Elkouss D, et al. QKD in standard optical telecommunications networks. In: Sergienko A, Pascazio S, Villoresi P, eds. *Quantum Communication and Quantum Networking*. Berlin: Springer, 2010. 142–149
- 15 Tanenbaum A S. *Computer Networks*. 4th ed. Upper Saddle River: Pearson Education Inc, 2003. 31–37
- 16 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Piscataway: IEEE, 1984. 175–179
- 17 Hwang W Y. Quantum key distribution with high loss: toward global secure communication. *Phys Rev Lett*, 2003, 91: 057901
- 18 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys Rev Lett*, 2005, 94: 230503
- 19 Lo H K, Ma X F, Chen K. Decoy state quantum key distribution. *Phys Rev Lett*, 2005, 94: 230504
- 20 Brassard G, Salvail L. Secret-key reconciliation by public discussion advances. In: *Proceedings of Workshop on the Theory and Application of Cryptographic Techniques*, Lofthus, 1993. 410–423
- 21 Krawczyk H. LFSR-based hashing and authentication. In: *Proceedings of 14th Annual International Cryptology Conference*, Santa Barbara, 1994. 129–139
- 22 Wegman M N, Carter L. Universal classes of hash functions. *J Comput Syst Sci*, 1979, 18: 143–154
- 23 Wegman M N, Carter L. New hash functions and their use in authentication and set equality. *J Comput Syst Sci*, 1981, 22: 265–279
- 24 Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photonics*, 2010, 4: 686–689

Field application and security management of a telephone network and a high speed data transmission system with practical fiber quantum cryptography

WU Hua^{1†}, ZHAO YuKang^{2†}, ZHAO Yong^{2,3,4} & ZHAO MeiSheng^{4*}

1 *The School of Public Affairs, University of Science and Technology of China, Hefei 230026, China;*

2 *Hefei National Laboratory for Physical Science at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China;*

3 *Research Center for Quantum Technology and Application, Chinese Academy of Science, Jinan 250101, China;*

4 *Shandong Institute of Quantum Science & Technology Co., Ltd., Jinan 250101, China*

*E-mail: meisheng.zhao@quantum-info.com

†Contributed equally to this work

Abstract To show how the introduction of quantum communication technology to traditional communication system can meet the demand of field application and security management, we explained in detail the design of a fiber quantum communication system, taking a telephone network and a high speed data transmission system

as an example, both were encrypted with quantum cipher and were built on field fiber recently. The procedure of implement and long term operation result of this system were also briefly introduced. It has been verified that this system possessed good reliability and usability, while meeting the functional demand for various types of communication and high level security of critical events. We also made some proposals for introducing quantum communication system to public management.

Keywords quantum communication, quantum cryptography, network layers, network management, security of data

ZHAO YuKang was born in 1981. He is now a Ph.D. student in Hefei National Laboratory for Physical Science at Microscale, University of Science and Technology of China.

ZHAO Yong was born in 1980. He received the Ph.D. degree from Heidelberg University, Heidelberg, Germany, in 2009. He is now the vice director of the Center for Quantum Technology and Applied Research of the Chinese Academy of Sciences and the chief engineer of Shandong Institute of Quantum Science and Technology, Co. Ltd.

ZHAO MeiSheng was born in 1980. He received the Ph.D. degree from University of Science and Technology of China, Hefei, in 2007. He is now an engineer of Shandong Institute of Quantum Science and Technology, Co. Ltd.