基于无线通道的电力量子密钥分发系统

吴佳伟[1]，卞宇翔[2]，张庆[1]，冯宝[2]
（1. 国网上海市电力公司信息通信公司，上海 200030;
2. 南京南瑞国盾量子技术有限公司，江苏 南京 211000）

摘　要：针对传统基于光纤通道的密钥分发方式受限于光纤资源和建设成本，难以满足接入侧海量电力业务终端，特别是移动终端的安全提升需求。为此，提出了一种适用于电力系统海量业务终端的基于无线信道的量子密钥分发系统。基于电力系统海量业务终端无线接入需求，给出了基于无线信道的电力量子密钥分发系统总体设计，从量子安全服务控制平台、量子密钥存储管理平台、海量电力业务终端平台 3 个方面详细分析了基于无线信道的电力量子密钥分发系统的功能模块及执行流程。在此基础上，结合用电信息采集、移动办公等典型电力业务，全面分析了基于无线信道的量子密钥分发系统应用于海量电力业务终端场景的优势和前景。

关键词：量子保密通信；无线信道；量子密钥分发；海量业务终端
中图分类号：TP393
文献标识码：A
doi:10.11959/j.issn.1000−0801.2020031

Wireless quantum power distribution system based on wireless

WU Jiawei[1], BIAN Yuxiang[2], ZHANG Qing[1], FENG Bao[2]
1. Information and Communication Company, State Grid Shanghai Electric Power Company, Shanghai 200030, China
2. NRGD Quantum CTEK Co., Ltd., Nanjing 211000, China

Abstract: The traditional optical fiberchannel-based key distribution method is limited by the optical fiber resources and construction cost, and it is difficult to meet the security enhancement requirements of the access side massive power service terminals, especially the mobile terminals. In this respect, a wireless channel-based quantum key distribution system was proposed, which was suitable for mass service terminals of power systems. Based on the wireless access requirements of mass service terminals in power system, the overall design of power quantum key distribution system based on wireless channel was given. The functional modules and execution flow of the power quantum key distribution system based on wireless channel were analyzed in detail from three aspects: quantum security service control platform, quantum key storage management platform and massive power service terminal platform. On this basis, combined with the typical power service such as electricity information collection and mobile office, the advantages and prospects of the quantum channel distribution system based on wireless channel applied to the terminal scenario of massive power service were comprehensively analyzed.

Key words: quantum secure communication, wireless channel, quantum key distribution, mass service terminal

收稿日期：2019−10−18；修回日期：2020−01−19
基金项目：面向城市能源互联网的新型量子通信网络建设和业务应用验证项目（No.B246MI190002）
Foundation Item: Construction of New Quantum Communication Network and Business Application Verification Project for Urban Energy Internet (No.B246MI190002)

1　引言

量子保密通信技术基于量子力学的基本原理，不依赖于计算复杂性，不会受到计算能力和数学水平提高的威胁，从理论上可以保证数据的安全传输。量子密钥分发具有绝对的随机性，具有理论上的无条件安全性，一旦存在窃听就必然被发现[1-3]。因此，量子保密通信是当前已知唯一的具有长期安全性保障的安全通信解决方案。

电力网络是支撑国家产业发展和民生稳定的重要基础。随着智能电网、能源互联网的发展，电网与用户双向互动性增强，大规模用户侧接入、智能采集终端和移动作业终端的广泛应用、黑客攻击等现状对电网发展提出了新的挑战和风险，电网安全防护和安全保障的压力、难度持续增加，迫切需要推进以量子保密通信技术为代表的新一代安全防御技术的研究应用，以尽快构建新型的、更可靠的下一代电网安全防护体系，全面提升安全防护技术和能力[4]。

当前，基于量子保密通信技术的电力业务承载，普遍采用裸光纤信道进行密钥分发，技术成熟度较高，应用范围较广。但是对于光纤难以覆盖的海量电力业务终端，一方面受限于纤芯资源，另一方面受限于成本，难以直接采用光纤信道进行量子密钥分发。基于无线通道的量子密钥分发技术则可以实现海量电力业务终端的量子保密通信安全提升。采用基于无线通道的量子密钥分发技术，实现了对现有通信方式安全性的大幅提升[5]，可以节约大量的光纤资源，提高网络运行的经济性，大幅降低建设成本，具有较大的技术优势。

2　量子密钥分发基本原理

依据量子力学的物理特性，量子密钥分发（quantum key distribution，QKD）在发送者和接收者之间通过量子信道传输编码信息的量子态，可在合法用户间建立安全的通信密钥，并从物理机制上保证其安全性，提供对窃听者的可检测性[6]。QKD 协议的理论方案包含两个部分，第一部分包括数据的编码、传输、解码，目的是为了在两个用户之间建立共享数据，又称筛选密钥；第二部分是通过误码率估计检测已有的传输过程是否遭到窃听，如果结果表明传输过程没有被窃听，则可通过信息方处理后可获得安全的密钥。

BB84 协议是最早、最典型也是目前应用最为广泛的量子密钥分发协议。该协议由 BENNET C H 和 BRASSARD G[7]于 1984 年提出，利用光子的偏振态编码信息。因为光子的偏振有两个相互线性独立的自由度（即偏振态相互垂直），所以信息的发送者和接收者可以简单选取“横竖基”，即“＋”，和“对角基”，即“×”，作为测量光子偏振的基矢。

基于 BB84 协议，横竖基中偏振方向“↑”代表 0，偏振方向“→”代表 1；对角基中偏振方向“↗”代表 0，偏振方向“↘”代表 1。传输一组二进制信息时，发送者对每个比特随机选一个基矢，即“＋”或者“×”，然后把每个比特（在各自被选的基矢下）对应的偏振光子发送给接收者。光子通过不破坏偏振态的（保偏）光纤或者自由空间传输到接收者。接收者对接收到的每个比特随机选择“＋”或者“×”基来测量。在测量出所有的 0 和 1 后，接收者和发送者之间要通过经典信道比对各自用过的基矢，然后保留相同的基矢，舍弃不同的基矢，获得筛选密钥，即原始量子密钥。最后，在传输不被窃听条件下，通过信息后处理，获得安全的量子密钥。

BB84 协议量子密钥的分发过程如下：

步骤 1　Alice 产生一个偏振光子序列并发送给 Bob；

步骤 2　Bob 接受 Alice 发送过来的每一个偏振光子，并随机选择基矢进行测量，记录下测量结果；

步骤 3　Bob 公开对每一个偏振光子的测量基，但不公开测量结果；

步骤 4 Alice 和 Bob 保留所有测量正确的测量基，并将左旋和水平记录为“0”，将右旋和垂直记录为“1”，这样 Alice 和 Bob 具有相同的量子密钥。

发送方 Alice 准备用于发送量子序列的量子源和一个随机比特序列，Alice 根据比特序列依次随机选择基矢制备 1 个量子态，并将量子态序列，发送给接收方 Bob；接收方 Bob 并不清楚 Alice 使用哪个基矢制备的量子态，因此也随机选择一个基矢对接收到的量子态进行测量，并记录测量结果。在量子序列发送后，Alice 公布制备量子态时选择的基矢序列，Bob 对基矢序列进行比对，舍弃了不同基矢的测量结果，余下的比特信息经过“后处理”过程后就作为双方共享的量子密钥，从而完成了量子密钥的分发过程。

3 基于无线通道的电力量子密钥分发系统设计

3.1 方案总体设计

无线通道特指从发射端到接收端没有一个诸如光纤、网线的有形连接，而是以电磁信号的形式进行数据传播。基于无线通道的电力量子密钥分发系统包括 3 个组成部分，分别是量子安全服务控制平台[8]、量子密钥存储管理平台和海量电力业务终端平台。量子安全服务控制平台承载了量子密钥无线分发服务器（quantum key wireless distribution server，QKWDS），是量子密钥生成与无线分发的核心系统。量子密钥存储管理平台包含量子密钥充注机（quantum key filling machine，QKFM），实时补充量子密钥，并为量子 TF 卡、量子 Ukey 等无线介质充入量子密钥，以供海量移动终端等设备使用。海量电力业务终端平台是使用量子密钥的海量电力业务终端，插入量子 TF 卡、量子 Ukey 等无线介质即可使用量子密钥。

基于无线通道的电力量子密钥分发系统总体设计如图 1 所示。

基于无线通道的电力量子密钥分发系统设计需要依托量子密钥充值系统。量子密钥充值系统主要包括量子密钥无线分发系统、量子密钥充注机[9]以及量子 Ukey 或安装量子 TF 卡的手机终端、笔记本终端、办公电脑终端、集中器等业务终端。其中，量子 Ukey 或量子 TF 卡通过量子密钥充注机获取密钥后，使用量子密钥进行身份认证，通过量子 SSL VPN（secure socket layer virtual private network，安全套接层虚拟专用网）网关[10]建立安全通道，接入内网，访问相关应用服务器。量子密钥充值系统方案设计如图 2 所示。

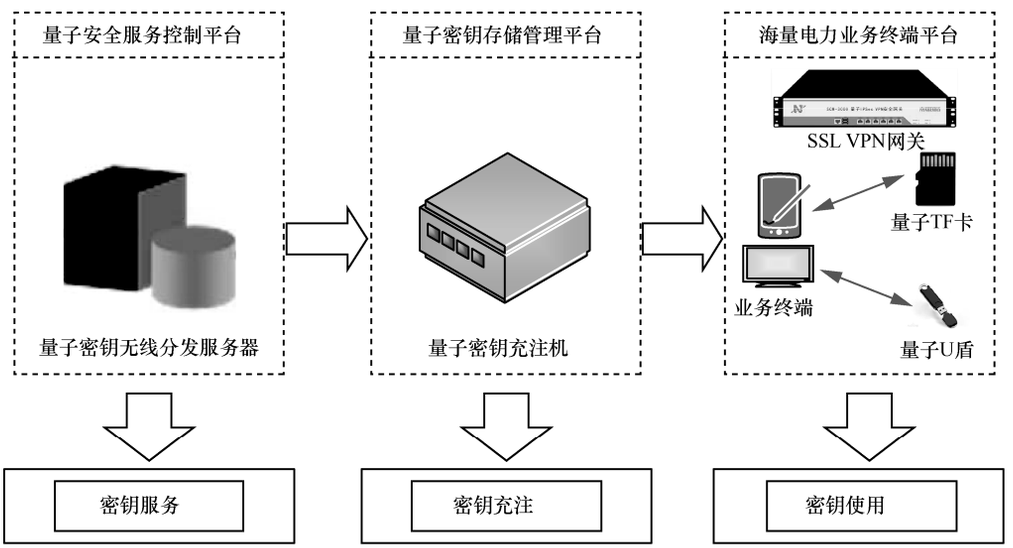


图 1 量子密钥无线分发系统总体设计

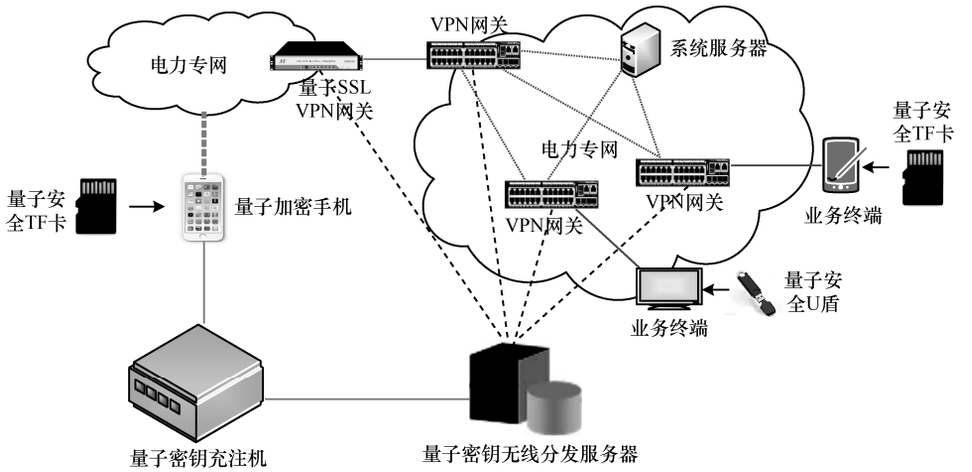


图 2　量子密钥充注系统方案示意图

3.2　量子安全服务控制平台

量子安全服务控制平台（quantum security service control center，QSSCC）包括量子密钥安全服务（quantum key security service，QKSS）和量子密钥分发服务（quantum key distribution service，QKDS）两个服务模块以及量子密钥无线分发服务器 QKWDS，QSSCC 的技术架构如图 3 所示。QSSCC 是基于 QKD[11]网络建立的量子密钥应用服务平台。作为 QKD 网络的扩展和延伸，量子密钥无线分发服务器 QKWDS 将量子密钥资源通过量子 TF 卡、量子 Ukey 融合到各种移动通信设备中，同时对移动密钥进行动态管理，为用户提供任意多点间密钥协商、接入认证、访问控制、安全存储等功能服务。

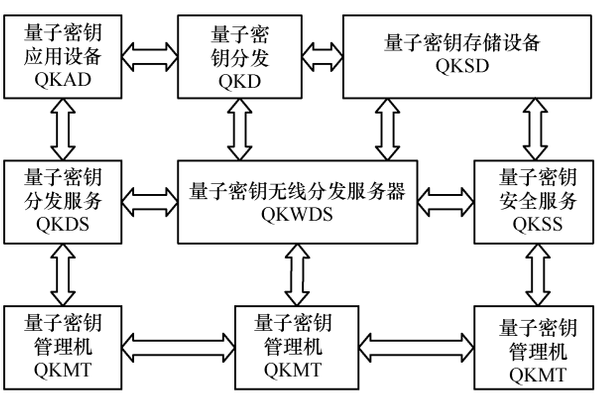


图 3　量子安全服务控制平台整体架构

3.2.1　量子密钥安全服务

量子密钥安全服务 QKSS 是量子密钥无线分发服务器 QKWDS 系统的中心站点，存储、管理着整个系统中成对出现的量子密钥资源，是量子密钥应用网络的认证和密钥管理中心，为接入网络中的设备提供量子会话密钥的分发服务，具有如下特性。

（1）接入认证及访问控制：对访问系统的移动终端进行安全认证和访问控制，授权在许可的生命周期内提供量子会话密钥的分发服务。

（2）多点间密钥协商：为已认证的多个移动终端及服务器端，提供量子会话密钥分发服务。

（3）密钥安全存储：提供量子密钥安全存储服务，存储设备配置专用加密芯片，以密文状态保存。

（4）提供加/解密服务：支持基于量子密钥的 SM1、SM3、SM4 等国家密码局标准算法进行加解密服务[12]。

（5）为量子密钥存储设备（quantum key storage device，QKSD）提供量子密钥更新的接口。

（6）量子安全设备管理服务：提供包括量子安全介质和量子可信设备管理服务，内容包含权限管理、生命周期管理等。

3.2.2　量子密钥分发服务

量子密钥分发服务 QKDS 位于量子密钥应用

站点内，与 QKD 网络中的量子密钥管理机（quantum key management terminal，QKMT）[13]对接，为站点内的量子密钥应用设备（quantum key application device，QKAD）提供量子会话密钥分发服务。其具有如下特性。

- QKDS 是 QKAD 对 QKWDS 的一个访问入口，对访问的 QKAD 进行认证，并将认证信息传递到 QKWDS 中心。
- QKDS 能向 QKAD 提供量子会话密钥分发服务接口。
- QKDS 能向 QKAD 提供使用量子会话密钥进行加解/密的接口。
- QKDS 适用于量子密钥应用站点和 QKWDS 中心（子密钥分发服务可部署在 QKWDS 中心，为 QKWDS 中心内的量子密钥应用设备提供量子会话密钥分发服务）[14]。
- QKDS 以协议接口的形式提供。

3.3 量子密钥存储管理平台

量子密钥存储管理平台的核心是量子密钥充注机，量子密钥充注机是量子无线密钥分发的重要基础设施，具有量子安全模块识别认证和量子密钥充注功能[15]，可以有效提高量子密钥充注的便利性。量子密钥充注机是量子密钥资源的“续航站”，量子 TF 卡、量子 Ukey 等安全介质可以通过量子密钥充注机安全可信地就近接入量子网络，更新量子密钥资源，为量子移动安全续航。量子密钥充注机的主要功能有：

- 合法接入量子保密通信网络，安全获取量子密钥资源；
- 实现用户合法性、密钥保密性以及信息完整性的安全设计，安全地提供用户量子密钥充注功能；
- 提供量子 Ukey、量子 TF 卡等安全介质的设备管理。

3.4 海量电力业务终端平台

海量电力业务终端平台的核心是量子 TF 卡或量子 Ukey 等无线介质。量子 TF 卡，在满足移动智能设备外扩存储需求的基础上，扩展了量子移动安全应用接口，提供用户增值的量子移动安全服务。量子 Ukey 采用高性能专用安全处理芯片，并与量子密钥无线分发技术紧密结合，提供高速的量子密钥应用接口，数据传输速度快、存储容量大、安全性高。

3.4.1 量子 TF 卡

量子 TF 卡密钥读取模式包括主动模式、被动模式[17]两类。

（1）主动模式

由终端通过 TF 定制接口协议主动发送分组请求，量子 TF 卡对身份信息认证完成后，一次提取所有的密钥池存储于本地安全模块的加密区域内。

（2）被动模式

量子 TF 卡按照设定的规则，通过接口协议定时向终端获取随机数，终端身份信息完成后，检查存储的随机数是否有效，有效的情况下反馈给量子 TF 卡，量子 TF 卡根据随机数将密钥发送至终端。

3.4.2 量子 Ukey

量子 Ukey 的密钥读取模式包括主动模式、被动模式[18]两类。主动模式是由终端通过量子 Ukey 定制接口协议主动发送分组请求，量子 Ukey 对身份信息认证完成后，一次提取所有的密钥池存储于本地安全模块的加密区域内；被动模式是量子 Ukey 按照设定的规则，通过接口协议定时向终端获取随机数，终端身份信息完成后，检查存储的随机数是否有效，有效的情况下反馈给量子 Ukey，量子 Ukey 根据随机数将密钥发送至终端。

4 典型应用

根据本文设计的基于无线通道的电力量子密钥分发系统，提出其在用电信息采集和移动办公两类电力业务的典型应用，展示无线量子密钥分

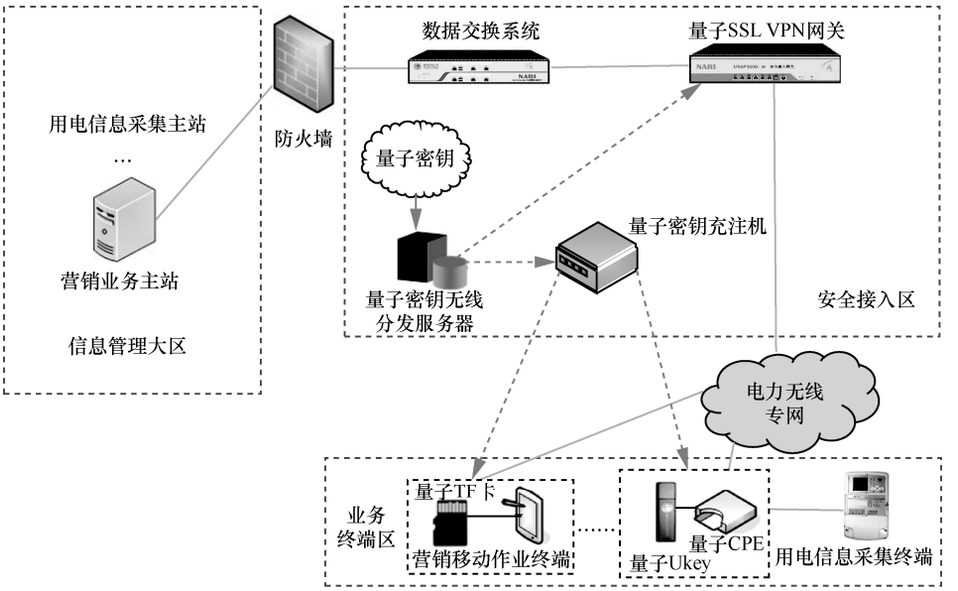


图 4　基于无线通道的电力量子密钥分发系统的用电信息采集业务应用架构

发技术在海量电力业务终端应用的优势和前景。

4.1　用电信息采集业务

用电信息采集业务主要包括信息管理大区、安全接入区、业务终端区 3 个部分。其中，在安全接入区实现量子安全服务控制平台和量子密钥存储管理平台的接入，部署量子密钥无线分发服务器、量子 SSL VPN 网关、量子密钥充注机等相关设备。安全接入区通过数据交换系统及防火墙与信息管理大区的用电信息采集主站等营销业务主站相连。同时安全接入区通过电力无线专网与业务终端区通信。业务终端区包含营销移动作业终端、量子 CPE、用电信息采集终端等相关设备。基于无线通道的电力量子密钥分发系统的用电信息采集业务应用架构如图 4 所示。

基于无线通道的电力量子密钥分发系统的用电信息采集业务加解密过程首先是用电信息采集业务终端以及量子 Ukey 或量子 TF 卡在量子密钥无线分发服务器上进行注册和身份认证，获取访问量子密钥无线分发服务器的密钥凭证[16]。量子 TF 卡、量子 Ukey 在量子密钥充注机进行密钥充注，从而获取量子密钥，再将量子 TF 卡、量子 Ukey 插入业务终端区海量的用电信息采集业务终端进行密钥使用，通过量子 SSL VPN 网关和电力无线专网完成用电信息采集业务数据的加/解密。同时，用电信息采集业务终端可以通过量子 Ukey 或量子 TF 卡在密钥充注机实现密钥更新。

4.2　移动办公业务

针对移动办公业务场景，同样可以应用基于无线通道的电力量子密钥分发系统应用。技术应用路线与用电信息采集业务基本一致，此处不再赘述。基于无线通道的电力量子密钥分发系统的移动办公业务应用架构如图 5 所示。

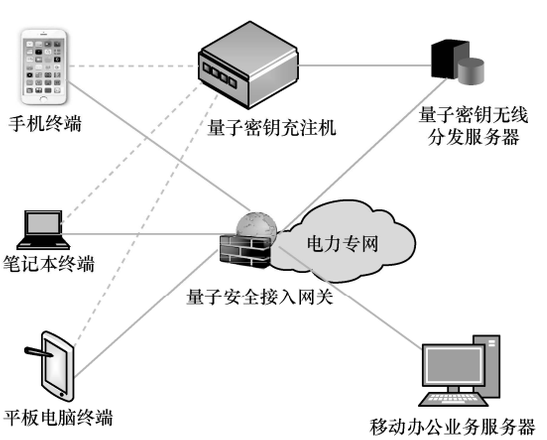


图 5　基于无线通道的电力量子密钥分发系统的移动办公业务应用架构

测试基于无线通道的电力量子密钥分发系统的移动办公业务应用情况。打开各类手机、笔记本、平板电脑等移动终端，并在量子密钥无线分发服务器上完成注册和身份认证。插入量子 TF 卡或量子 Ukey，查看移动终端的密钥量。使用移动终端 A 和移动终端 B 进行移动办公业务模拟仿真，移动办公业务结束后查看移动终端的密钥使用情况。测试结果发现，采用量子密钥进行移动办公业务数据加密不影响移动终端的正常使用，移动办公业务运行正常，同时量子密钥在移动办公业务模拟仿真过程中被使用，相关移动办公业务数据被量子密钥严格加密，起到了安全保护的作用。其中，移动终端 A 和 B 的密钥量使用前后见表 1。

表 1　移动办公业务密钥消耗情况

阶段	移动终端 A/byte	密钥消耗/byte	移动终端 B/byte	密钥消耗/byte
移动终端系统登录前	21 685 189		21 685 189	
移动终端系统登录后	21 684 677	512	21 684 677	512

5　结束语

量子安全服务控制平台承载了量子密钥无线分发服务器，是量子密钥生成与无线分发的核心系统。量子密钥存储管理平台包含了量子密钥充注机，实时补充量子密钥，并为量子 TF 卡、量子 Ukey 等无线介质充入量子密钥，以供海量移动终端等设备使用。海量电力业务终端平台是使用量子密钥的海量电力业务终端，插入量子 TF 卡、量子 Ukey 等无线介质即可使用量子密钥。相比于传统基于光纤密钥分发方式，本文提出的基于无线通道的电力量子密钥分发系统可以便捷地提高海量电力业务终端的安全性，技术先进性十分明显，应用场景十分广阔。

参考文献：

[1] 康双勇. 量子通信技术发展现状及研究进展[J]. 保密科学技术, 2017(3): 7-10.
KANG S Y. Development status and research progress of quantum communication technology[J]. Security Science and Technology, 2017(3): 7-10.

[2] 杨旻. 新时期量子通信技术发展现状及发展趋势探讨[J]. 中国高新科技, 2017, 1(3): 35-37.
YANG M. Discussion on the development status and development trend of quantum communication technology in the new era[J]. China High Technology, 2017, 1(3): 35-37.

[3] 陈智雨, 郝悍勇, 王栋, 等. 电力量子保密通信实用化技术研究进展与展望[J]. 电力信息与通信技术, 2018, 16(4): 15-23.
CHEN Z Y, HAO H Y, WANG D, et al. Research progress and prospect of practical technologies for quantum secure communication[J]. Electric Power Information and Communication Technology, 2018, 16(4): 15-23.

[4] 于秋生, 马超, 周洁. 量子通信技术在电力通信方面应用展望[J]. 山东工业技术, 2016(24): 176.
YU Q S, MA C, ZHOU J. Application prospect of quantum communication technology in power communication[J]. Shandong Industrial Technology, 2016(24): 176.

[5] 樊矾, 魏世海, 杨杰, 等. 量子保密通信技术综述[J]. 中国电子科学研究院学报, 2018, 13(3): 356-362.
FAN F, WEI S H, YANG J, et al. Summary of quantum secure communication technology[J]. Journal of China Academy of Electronics and Information Technology, 2018, 13(3): 356-362.

[6] 任媛媛. 量子通信技术的发展及其应用前景[J]. 安徽科技, 2016(10): 53-56.
REN Y Y. Development and application prospect of quantum communication technology[J]. Anhui Science and Technology, 2016(10): 53-56.

[7] 陈晖, 何远杭, 黎珂, 等. 量子密钥服务及移动应用技术[J]. 中国电子科学研究院学报, 2018, 13(4): 406-409, 414.
CHEN H, HE Y H, LI K, et al. Quantum key service and mobile application technology[J]. Journal of China Academy of Electronics and Information Technology, 2018, 13(4): 406-409, 414.

[8] 赖俊森, 吴冰冰, 李少晖, 等. 量子保密通信研究进展与安全性分析[J]. 电信科学, 2015, 31(6): 46-52.
LAI J S, WU B B, LI S H, et al. Research progress and security analysis of quantum secure communication[J]. Telecommunications Science, 2015, 31(6): 46-52.

[9] 张翼英, 张素香. 量子通信及其在电力通信的应用[J]. 电力信息与通信技术, 2016, 14(9): 7-11.
ZHANG Y Y, ZHANG S X. Quantum communication and its application in power communication[J]. Electric Power Information and Communication Technology, 2016, 14(9): 7-11.

[10] 严晓玲, 江冬娜. 量子通信技术及其在电力系统中的应用分析[J]. 通讯世界, 2015(21): 8-9.
YAN X L, JIANG D N. Analysis of quantum communication technology and its application in power system[J]. Communications World, 2015(21): 8-9.

[11] 罗彬. 量子通信及其在电力通信的应用[J]. 电子测试, 2018(20): 76-77.
LUO B. Quantum communication and its application in power communication[J]. Electronic Test, 2018(20): 76-77.

[12] 叶志远, 陈华智, 王文清. 量子密钥分发保密通信系统电力应用方向探讨[J]. 工程建设与设计, 2016(8): 238-239.
YE Z Y, CHEN H Z, WANG W Q. Discussion on the power application direction of quantum key distribution secure communication system[J]. Engineering Construction and Design, 2016(8): 238-239.

[13] 刘晓慧, 裴昌幸, 聂敏. 量子无线通信网络构建及性能分析[J]. 吉林大学学报(工学版), 2014, 44(4): 1177-1181.
LIU X H, PEI C X, NIE M. Construction and performance analysis of quantum wireless communication network[J]. Journal of Jilin University (Engineering & Technology Edition), 2014, 44(4): 1177-1181.

[14] 王磊, 赵广怀, 范晓楠, 等. 量子保密通信在电网业务应用的方案研究与设计[J]. 电力信息与通信技术, 2018, 16(3): 34-38.
WANG L, ZHAO G H, FAN X N, et al. Scheme research and design of quantum secret communication in power grid business applications[J]. Electric Power Information and Communication Technology, 2018, 16(3): 34-38.

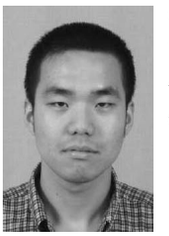
[15] 曹原, 赵永利, 郁小松, 等. 量子密钥分发驱动安全电力通信网络体系架构[J]. 中国电力, 2017, 50(10): 8-11, 34.
CAO Y, ZHAO Y L, YU X S, et al. Quantum key distribution drives secure power communication network architecture[J]. China Electric Power, 2017, 50(10): 8-11, 34.

[16] 张沛, 周小清, 李智伟. 基于量子隐形传态的无线通信网络身份认证方案[J]. 物理学报, 2014, 63(13): 27-32.
ZHANG P, ZHOU X Q, LI Z W. Identification scheme of wireless communication network based on quantum teleportation[J]. Acta Physical Sinica, 2014, 63(13): 27-32.

[17] 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.
MIAO C H, WANG J F, WEI S H, et al. Design of mobile terminal encryption scheme based on quantum key[J]. Network Security Technology and Application, 2018(6): 38, 44.

[18] 王健全, 马彰超, 李新中, 等. 量子保密通信网络架构及移动化应用方案[J]. 电信科学, 2018, 34(9):10-19.
WANG J J, MA Z C, LI X Z, et al. Quantum secure communication network architecture and mobile application scheme[J]. Telecommunications Science, 2018, 34(9): 10-19.

[作者简介]



吴佳伟（1981– ），男，国网上海市电力公司信息通信公司高级工程师、工程中心副主任，主要从事电力系统通信建设及运行维护等工作。

卞宇翔（1990– ），男，南京南瑞国盾量子技术有限公司工程师、销售工程部项目经理，主要从事量子保密通信技术研究等工作。

张庆（1966– ），男，国网上海市电力公司信息通信公司高级工程师、安全监察部主任，主要从事量子保密通信技术研究等工作。

冯宝（1984– ），男，南京南瑞国盾量子技术有限公司高级工程师、销售工程部经理，主要从事量子保密通信技术研究等工作。