



专题:信息安全

量子保密通信研究进展与安全性分析

赖俊森, 吴冰冰, 李少晖, 赵文玉, 张海懿

(中国信息通信研究院通信标准研究所 北京 100191)

摘要:量子保密通信基于量子密钥分配和“一次一密”加密体制,能够提供无条件安全性保证,成为学术界和产业界研究关注的焦点。在介绍量子保密通信协议原理、关键器件和网络架构的基础上,重点分析了实际量子密钥分配系统的安全漏洞、攻击手段和安全性对策以及测量设备无关量子密钥分配技术研究进展,并对量子保密通信技术的安全性挑战、发展方向和应用前景进行了展望。

关键词:量子保密通信;量子密钥分配;安全性分析

doi: 10.11959/j.issn.1000-0801.2015142

Progress and Security Analysis of Quantum Cryptography Communication

Lai Junsen, Wu Bingbing, Li Shaohui, Zhao Wenyu, Zhang Haiyi

(Communications Standards Research Institute, China Academy of Information and Communication Technology (CAICT), Beijing 100191, China)

Abstract: Quantum cryptography communication, which provided unconditional security by means of quantum key distribution and one-time pad encryption, has become one focus of communication academia and industry. The quantum key distribution protocol, devices, and network architecture were reviewed. The security loopholes and quantum hacking schemes of practical system were analyzed. Corresponding security countermeasures were summarized. Recent progress of measurement-device-independent quantum key distribution was also introduced. In the end, the security challenge, development direction and prospects of quantum cryptography communication were also discussed.

Key words: quantum cryptography communication, quantum key distribution, security analysis

1 引言

随着电子商务、移动支付和互联网金融等新兴业务的

高速发展,网络通信技术已经深入影响到当今社会和经济生活的各个方面。而近来不断曝光的监控窃听丑闻和用户隐私泄露事件更是加剧了学术界和产业界对于互联网网

收稿日期:2014-12-02;修回日期:2015-06-09

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(No.2013AA013402, No.2015AA015502),国家自然科学基金资助项目(No.61171076, No.61201260, No.61471128)

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2013AA013402, No.2015AA015502), The National Science Foundation of China (No.61171076, No.61201260, No.61471128)

论文引用格式: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.电信科学,2015142

Lai J S, Wu B B, Li S H, *et al.* Progress and security analysis of quantum cryptography communication. Telecommunications Science, 2015142

络信息安全的忧虑和关注。传统保密通信技术借助加/解密算法的数学复杂度提供有限的计算安全性(computational security),随着分布式计算和量子计算机技术的发展,传统保密通信技术的安全性将面临严重挑战^[1]。

1949 年,香农从理论上证明了“一次一密(OTP)”密码体制通过采用与明文等长(相同速率)的完全随机密钥对明文进行逐比特加密,在密钥安全共享的前提下,可以提供保密通信的无条件安全性(unconditional security)^[2]。而量子密钥分配(QKD)依据量子力学中的不确定性原理、测量坍缩原理和未知量子态不可克隆原理,能够为通信双方提供不可被窃听、存储和破解的量子密钥安全共享信道^[3]。结合了 QKD 技术和 OTP 密码体制的量子保密通信技术作为量子信息领域最为成熟和实用化的技术,能够在保密通信中提供理论上的无条件安全性,受到学术界和产业界越来越多的研究和关注^[4-8]。

本文首先介绍量子保密通信系统的协议原理、关键器件和网络架构,其次分析现实 QKD 系统存在的安全漏洞、攻击手段和安全性对策,之后关注测量设备无关量子密钥分配(MDI-QKD)技术研究进展,最后给出对于量子保密通信技术发展方向、安全性挑战和应用前景的分析与展望。

2 量子保密通信技术研究进展

在量子保密通信中应用最为广泛的基于准单光子脉冲调制的诱骗态 BB84 协议 QKD 系统,如图 1 所示^[3]。BB84 协议以不同量子态表征经典通信中的二进制比特,发射端 Alice 在量子随机数生成器(QRNG)控制下随机选择直角或斜角测量基矢对弱相干光脉冲(WCP)进行偏振或相位调制,同时为了避免窃听者 Eve 可能采取针对准单光子源的光子数分离(PNS)攻击,发射端还进行光脉冲强度随机切换的诱骗态调制^[9],接收端 Bob 同样采用随机基

矢进行光脉冲偏振或相位测量,并丢弃不匹配基矢测量结果,通过与 Alice 公布的测量基矢进行抽取对照和纠错放大,计算误码率和多光子脉冲数的上限值,排除 PNS 攻击,最终提炼出双方的共享密钥,并对通信明文进行 OTP 加密^[10]。诱骗态方案解决了 WCP 的准单光子源安全问题,为量子保密通信走向实用化铺平了道路^[11-14]。

量子保密通信协议的研究进展包括:以简化系统配置为目标的分布式相位参考 QKD 协议^[15],通过对相邻光脉冲的差分相位编码和接收端自相关检测实现密钥分配,适用于传输距离小于 100 km 的 QKD 系统;以提高安全传输距离为目标的基于量子纠缠对 QKD 协议^[16],利用自发参量下变换光源产生偏振纠缠光子对,能够容忍更高的信道损耗(约 70 dB),但量子纠缠对制备困难,退相干效应明显,成码率较低;以提高量子态检测效率为目标的连续变量 QKD 协议^[17]利用相干零差或外差探测对光场复空间进行量子信息编码和测量,无需单光子探测,易于与现有光纤通信系统集成,但对于信道损耗敏感,与强光信号混传受限。

在量子保密通信系统中,WCP 光源、单光子探测器和 QRNG 等关键器件对于安全成码率和传输距离等性能指标具有重要影响。鉴于量子点光源和分子晶体光源等单光子源技术尚不成熟,集成诱骗态调制的 WCP 光源仍是首选。在激光器内部集成幅度开关可以提高消光比,降低无光子脉冲数量,从而增大安全码率,使用单一激光器可以避免光脉冲特性差异带来的安全漏洞,光脉冲重复频率最高可达 100 MHz^[18]。在单光子探测器方面,现有光电倍增管和雪崩光电二极管的检测带宽、探测效率和暗计数率等指标受限明显,超导纳米线单光子探测器(SNSPD)成为重要发展方向,通过低温超导材料纳米线结构吸收光子产生电脉冲信号,可以实现超过 90%的探测效率、吉赫兹量级检测带宽和低于百赫兹的暗计数率^[19],但-270℃左右低温运

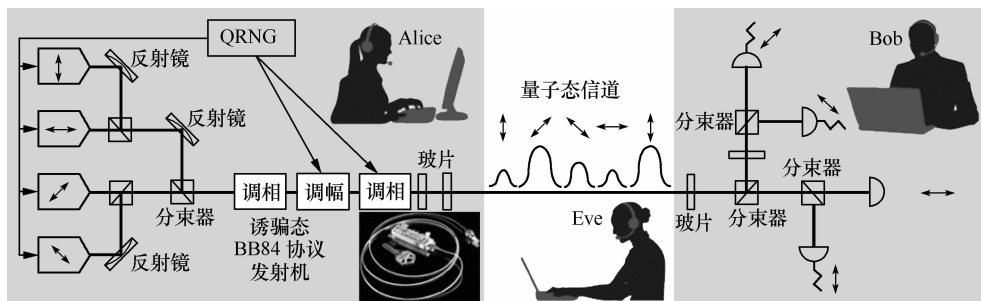


图 1 基于偏振调制的诱骗态 BB84 协议 QKD 系统原理^[3]



行条件是该类型器件应用推广的主要障碍。传统 QNRG 采用单光子分束检测方法,随机数生成速率较低,限制了 QKD 系统的最大带宽,而采用光放大器真空态量子噪声随机采样测量可以实现高速量子随机数生成,完全随机数生成的最高码率可达 100 Mbit/s 量级^[20]。

QKD 量子保密通信系统的典型应用和网络架构如图2所示,包含 3 个网络层:QKD 密钥传输层、密钥管理层和应用加密层。QKD 密钥传输层基于安全授信节点构建,授信节点间的光纤传输距离小于百千米,QKD 系统在相邻节点之间保持百 kbit/s 速率的连续密钥传输。各节点的密钥信息通过密钥代理服务器(KMA)在密钥管理层进行提取、存储和重构,并进行 QKD 安全码率和信道误码率的监测以及节点密钥信息的更新和重用。同样位于密钥管理层的密钥管理服务器(KMS)根据 KMA 的节点密钥信息,对整个 QKD 保密通信网络的密钥进行管理与控制,实现任意节点间的密钥中继和传输。在应用加密层,通过使用各节点间共享的量子密钥,也可结合传统加密算法,能够为灵活接入的各种类型业务提供 OTP 加密的安全传输信道。用户无需接触 QKD 密钥传输层和密钥管理层,仅根据业务需要接入 QKD 网络应用加密层节点,实时获取并存储 KMS 提供的用于信息加密的密钥信息。

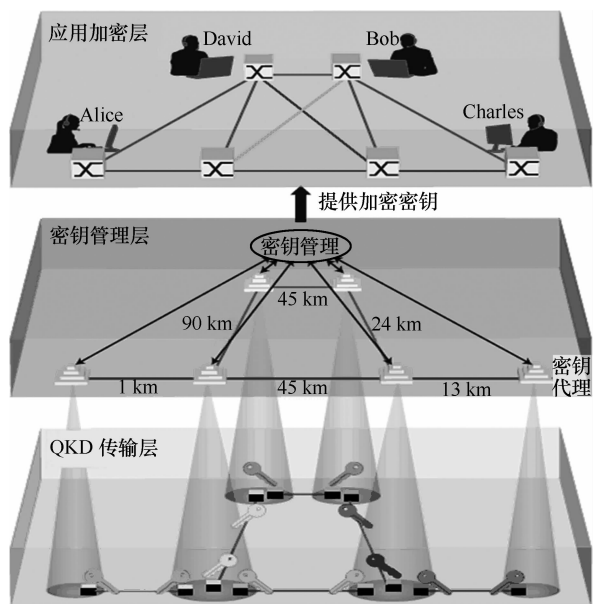


图2 典型量子保密通信系统网络架构^[21]

由于 QKD 量子保密通信存在协议编码的检测冗余、关键器件的性能局限以及安全授信节点的组网需求,目前实验系统的最高安全码率约为 2 Mbit/s (传输距离数十千

米),无可信中继节点的最大光纤传输距离约为 200 km (安全码率为数 kbit/s),主要面向城域范围的语音加密应用,难以满足现有光纤通信系统高速长距离传输加密的要求,同时 WCP 准单光子信号与传统强光信号的混合传输引入额外的耦合噪声,将进一步降低系统的性能^[3]。随着 WCP 光源、单光子探测器和 QRNG 等核心器件性能的提高以及编码协议方案的改进,QKD 量子保密通信系统将有望从现有的语音和低速数据加密传输应用逐步拓展到数据中心互联或干线传输等信息加密应用。

3 量子保密通信系统安全性分析

由量子力学原理保证安全性的 QKD 技术和对于密文攻击具有完善保密性的 OTP 加密体制相结合,为量子保密通信系统提供了理论和协议层面的无条件安全性。但是,实际 QKD 系统中光源、信道节点和接收机的不理想特性,使其难以满足理论模型的安全性证明要求,成为量子保密通信系统中可能被窃听者利用的安全漏洞。随着对量子保密通信系统研究的深入和商用化的推动,针对实际 QKD 系统的漏洞攻击和安全防御策略也成为该领域的研究热点。

针对光源和调制器的攻击主要包括:针对 WCP 多光子源的光子数分离攻击^[9],通过伪装信道损耗截获多光子脉冲中的部分同偏振光子来窃取密钥信息,可以通过诱骗态多强度调制监测信道误码率和多光子脉冲数的上限值来加以识别,还需要结合调制光强监控和多光源光谱校准保证其安全性。控制光源相位调制器延迟,降低 WCP 实际调制相位,进行相位重映射攻击^[21],在双向 QKD 系统中引入不越限误码率的情况下进行拦截重发,进而获取双方共享的密钥信息。

针对信道节点的攻击主要包括:利用全光纤 QKD 系统的光纤分束器分光比具有波长相关性,进行分束器波长攻击^[22],窃听者通过发送不同波长的伪脉冲改变测量分光比,并控制合法接收者检测基矢选择,在增加极低额外噪声条件下即可截获密钥信息。利用双向 QKD 系统中的偏振补偿角度偏差,进行被动法拉第反射镜攻击^[23],偏振补偿的不理想导致发送方公布的量子信号态增加了额外的希尔伯特空间维度,使得窃听者能够从中估计调制信息,并实施截取重发攻击。

针对单光子探测器的攻击主要包括:利用两组单光子探测器探测效率时域不匹配性,进行时移攻击^[24],通过随

机延迟改变 WCP 光子到达探测器的时间,使其位于探测效率不匹配点,即可改变接收测量基矢状态,并以一定概率窃取部分密钥。利用单光子探测器饱和线性工作模式的强光致盲攻击^[25],通过强光信号使工作于门模式的探测器在一定时段进行饱和和线性工作模式而致盲,无法响应单光子信号,窃听者截取线路光子,并分析出发送端的测量基矢,通过控制接收探测器响应,获取双方共享的所有密钥信息。利用探测器后脉冲效应产生的死时间进行探测器死时间攻击^[26],通过攻击脉冲使部分探测器处于死时间状态,控制接收端响应,并提高收发双方剩余光子的密钥状态重合率,进而获取密钥信息。

对于已知的 QKD 系统安全漏洞和攻击方式,可以采取相应的技术手段加以应对,例如通过诱骗态调制监测光子数分离攻击、利用探测器校准消除时移攻击以及借助不对称分束和监控信道防御强光致盲攻击等。但是,不断被发现的新的系统安全漏洞和攻击手段,使得现实 QKD 系统难以满足无条件安全性证明的假设,而对于整个 QKD 系统的动态特性和其中各个器件的非理想特性,进行分析和数学建模,以提供安全性证明的方法难以实现,所以完善和保证 QKD 系统的现实安全性成为量子保密通信技术发展的重要方向。

目前,现实 QKD 系统的安全性对策主要包括 3 个方面。首先,采用上文的系统攻防测试和安全补丁方法,针对已知的安全漏洞和攻击方法对系统进行改进升级,以提高安全性,但该方法无法防护潜在未知的系统漏洞和攻击,仅提供有限安全性保证。其次,采用设备无关量子密钥分配(DI-QKD)技术^[27],将量子态制备和测量装置均视为黑盒,不对量子信号的希尔伯特空间维度和检测方法等细节及其安全性进行假设,基于 Bell 不等式违背量函数观测,保证量子信息的相关性和安全性。DI-QKD 技术基于量子

物理定律又不依赖设备的物理状态和细节,能够提供完善的无条件安全性保证。但是,DI-QKD 对于联合 Bell 态测量过程中的单光子探测器检测效率要求(>80%)很高,并且需要量子比特放大或者公平采样技术辅助进行脉冲光子的非破坏测量,在现有技术条件下的安全成码率极低(约为 10^{-10} bit/脉冲),短期内难以实用化。最后,鉴于上述两种方案的局限性,2012 年 Lo 等人^[28]首次提出的测量设备无关量子密钥分配技术受到学术界和产业界的关注和重视。在 MDI-QKD 系统中,收发双方不进行任何测量,而是将 WCP 量子信号发送至安全不授信的第三方节点进行 Bell 态测量,并通过公开测量结果和安全授信检验提取共享密钥。与接收未知量子态的单光子探测器相比,收发双方用于制备量子信号的发射机处于相对封闭的可靠实验环境中,其安全性更易于保证。MDI-QKD 技术消除了所有探测器相关的安全漏洞,在发射机安全的前提下,能够基于现有的非理想器件和高损耗信道大幅增强 QKD 系统的安全性,从而提高整个量子保密通信系统的安全性和实用性。

4 测量设备无关量子密钥分配

量子保密通信技术的无条件理论安全性和 QKD 系统的现实安全性之间的差距,是量子保密通信推广实用的主要障碍之一,上述安全对策中的系统攻防测试临时性措施和短期内无法实用的 DI-QKD 技术,都难以保障 QKD 系统的现实安全性。MDI-QKD 方案基于现有的技术条件,消除了探测器相关的安全漏洞,能够有效提升量子保密通信系统的现实安全性,并且为 QKD 系统提供了穿越不授信网络节点的能力,为推动量子保密通信系统的研究和应用发展注入新的活力。

MDI-QKD 系统原理如图 3 所示,与传统 QKD 系统的

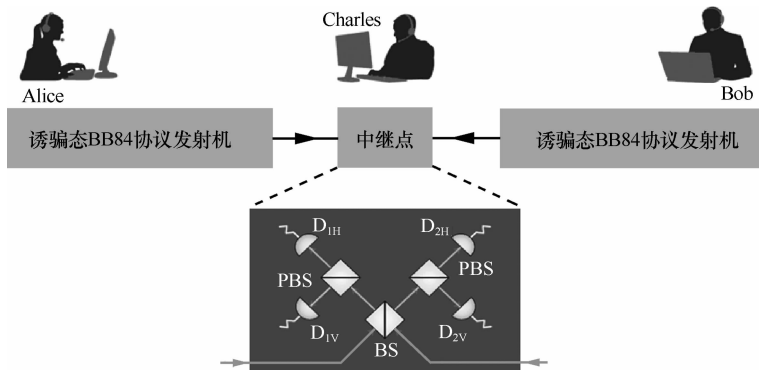


图 3 测量设备无关的量子密钥分配系统原理^[3]



一发一收机制不同,通信双方 Alice 和 Bob 均采用诱骗态 BB84 协议发射机,对相位随机的 WCP 进行随机基矢的偏振或相位调制,并将 WCP 量子信号发送至安全不授信中继节点 Charles(也可能是窃听者 Eve)处进行 Bell 态测量,依据网络中继节点公布的随机基矢测量结果进行授信认证和公共信道对基,保留相同基矢,并对比特编码进行翻转操作,最终获得双方共享密钥^[28]。

MDI-QKD 技术提出之后,在协议性能和系统实验等方面都得到了充分的分析和验证。在协议理论方面,Song 等人^[29]分析了实际脉冲源有限密钥长度条件下 MDI-QKD 系统的安全性问题,给出 MDI-QKD 系统与标准 BB84 协议系统安全码率下限的差异以及安全传输距离与 Bell 态测量有效事件数的正比关系。Ma 等人^[30]比较了不同诱骗态调制的 MDI-QKD 系统在低损耗和高损耗传输中的统计波动差异,指出了三强度诱骗态调制 MDI-QKD 系统在高损耗的优势。Wang 等人^[31]分析了发射机调制编码中的相位翻转误差对于 MDI-QKD 系统性能的影响,给出三强度诱骗态调制 MDI-QKD 系统的误码率估计算法,提升安全码率和传输距离。在系统实验方面,Ma 等人^[32]提出了基于相位编码的 MDI-QKD 实验系统方案,无需偏振和相位保持,仅采用两组单光子探测器进行 3 组测量基矢编码,并对该方案的组网传输能力进行分析。Silva 等人^[33]提出基于偏振调制的 MDI-QKD 系统,采用与传统电信系统兼容的 17 km 光纤波分复用系统进行自动偏振控制和发射机校准,三强度诱骗态调制生成码率为 10^{-6} bit/脉冲。Liu 等人^[34]采用长波泵浦参量上变换单光子探测器,在国际上首次实现了基于相位编码 MDI-QKD 系统的 25 kbit/s 安全码率 50 km 光纤传输,其中收发双方 WCP 相位调制需要保持光谱、定时和偏振态的一致性,并借助光纤反馈控制保证双方调制器干涉仪相位匹配,此外,还提出了星型 MDI-QKD 网络模型。

MDI-QKD 技术的最新研究进展还包括:对发射机 WCP 光源做出改进,采用基于量子干涉原理的改进相干光子源^[35]或奇相干光子源^[36],抑制光源中多光子脉冲的数量,从而提高诱骗态 MDI-QKD 系统的安全码率。结合现有的量子中继技术,在 MDI-QKD 系统的中继检测节点引入量子存储器^[37],通过单模存储量子中继增加系统可用传输距离^[38]。将连续变量量子密钥分配(CV-QKD)技术与 MDI-QKD 系统结合^[39],使用与标准光纤通信兼容的高斯相位调制光源和低成本高效率的相干平衡内差探

测器^[40]构建 CV-MDI-QKD 系统。

与诱骗态 BB84 协议 QKD 系统相比,MDI-QKD 系统的安全码率较低,原因在于中继节点对收发双方的量子脉冲信息进行 Bell 态测量,需要双倍的测量基矢吻合事件进行验证授信,这一缺点可以通过采用前述的高带宽和探测效率的 SNSPD 器件加以改进。

5 结束语

量子保密通信系统采用动态密钥实时分配的 QKD 技术和“一次一密”加密体制,为解决网络信息安全问题提供了具有无条件安全性保证的理想方案,但实际系统和器件的非理想特性给量子保密通信的现实安全性带来了挑战。BB84 协议的出现使量子保密通信从理论走向了现实,诱骗态调制技术解决了 WCP 多光子源的安全漏洞,为量子保密通信的实用化打开了大门,而 MDI-QKD 技术消除了探测器相关的所有安全漏洞,能够大幅提升量子保密通信的现实安全性和实用性。未来量子保密通信技术发展方向包括发展光源、探测器和量子中继技术,提高 QKD 系统的安全码率和可用传输距离,实现量子信号与传统光通信信号的光纤混合传输以及量子保密与传统保密的混合加密应用,进一步弥合 QKD 理论协议的无条件安全性和实际系统的非理想特性之间的差距。随着 MDI-QKD 技术的应用,针对量子保密通信系统的漏洞攻击将转向光源和发射机的安全漏洞,如偏振不一致性、相位分布特性和定时失配等,量子保密通信系统的现实安全性仍将是未来研究与应用的关注焦点,此外对于 MDI-QKD 系统的性能分析、系统验证和组网应用也有待于学术界和产业界持续和深入地研究和探索。

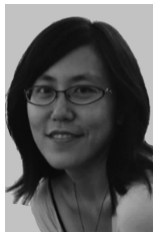
参考文献

- 1 Stinson D R. Cryptography: Theory and Practice, Third Edition. London: Chapman & Hall, 2005
- 2 Shannon C E. Communication theory of secrecy systems. Bell Sys Tech J, 1949, 28(4): 656~715
- 3 Lo H K, Curty M, Tamaki K. Secure quantum key distribution. Nature Photonics, 2014(8): 595~604
- 4 吴华, 王向斌, 潘建伟. 量子通信现状与展望. 中国科学: 信息科学, 2014, 44(3): 296~311
Wu H, Wang X B, Pan J W. Quantum communication: status and prospects. Science China: Information Sciences, 2014, 44(3): 296~311
- 5 李宏伟, 陈巍, 黄靖正等. 量子密码安全性研究. 中国科学: 物理学力学天文学, 2012, 42(11): 1237~1255

- Li H W, Chen W, Hang J Z, *et al.* Security of quantum key distribution. *Science China: Physics, Mechanics & Astronomy*, 2012, 42(11): 1237~1255
- 6 王金东, 张智明. 量子密钥分发系统的现实无条件安全性. *量子电子学报*, 2014, 31(4): 449~458
Wang J D, Zhang Z M. Unconditional security of quantum key distribution based on practical devices. *Chinese Journal of Quantum Electronics*, 2014, 31(4): 449~458
- 7 许华醒. 量子通信网络发展概述. *中国电子科学研究院学报*, 2014, 9(3): 259~271
Xu H X. Overview of quantum communication network development. *Journal of China Academy of Electronics and Information Technology*, 2014, 9(3): 259~271
- 8 徐兵杰, 刘文林, 毛钧庆等. 量子通信技术发展现状及面临的问题研究. *通信技术*, 2014, 47(5): 463~468
Xu B J, Liu W L, Mao J Q, *et al.* Development and problems of quantum communication technology. *Communications Technology*, 2014, 47(5): 463~468
- 9 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 2005, 94(23): 230503
- 10 Lo H K, Ma X, Chen K. Decoy state quantum key distribution. *Physical Review Letters*, 2005, 94(23): 230504
- 11 Peev M, Pacher C, Alleaume R, *et al.* The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 2009, 11(7): 075001
- 12 Chen T Y, Wang J A, Liang H, *et al.* Metropolitan all-pass and inter-city quantum communication network. *Optics Express*, 2010(18): 27217~27225
- 13 Stucki D, Legre M, Buntschu F, *et al.* Long-term performance of the swiss quantum quantum key distribution network in a field environment. *New Journal of Physics*, 2011, 13(12): 123001
- 14 Sasaki M, Fujiwara M, Ishizuka H, *et al.* Field test of quantum key distribution in the Tokyo QKD network. *Optics Express*, 2011(19): 10387~10409
- 15 Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution. *Physical Review Letters*, 2002, 89(3): 037902
- 16 Treiber A, Poppe A, Hentschel M, *et al.* Fully automated entanglement-based quantum cryptography system for telecom fiber networks. *New Journal of Physics*, 2009, 11(4): 045013
- 17 Jouguet P, Kunz J S, Leverrier A, *et al.* Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photon*, 2013(7): 378~381
- 18 Du H, Liang Y, Zhang S, *et al.* Practical high-speed light source for decoy-state quantum key distribution. *Chinese Optics Letters*, 2014, 12(7): 072702
- 19 Dauler E A, Grein M E, Kerman A J, *et al.* Review of superconducting nanowire single photon detector system design options and demonstrated performance. *Optical Engineering*, 2014, 53(8): 081907
- 20 Nie Y Q, Zhang H F, Zhang Z, *et al.* Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters*, 2014, 104(5): 051110
- 21 Xu F H, Qi B, Lo H K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 2010, 12(11): 113026
- 22 Huang J Z, Weedbrook C, Yin Z Q, *et al.* Quantum hacking of a continuous-variable quantum key distribution system using a wavelength attack. *Physical Review A*, 2013, 87(6): 062329
- 23 Sun S H, Jiang M S, Liang L M. Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. *Physical Review A*, 2011, 83(6): 062331
- 24 Zhao Y, Fung C H, Qi B, *et al.* Quantum hacking: experimental demonstration of time shift attack against practical quantum key distribution systems. *Physical Review A*, 2008, 78(4): 042333
- 25 Yuan Z L, Dynes J F, Shields A J. Avoiding the blinding attack in QKD. *Nature Photon*, 2010(4): 800~801
- 26 Weier H, Krauss H, Rau M, *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, 2011, 13(7): 073024
- 27 Masanes L, Pironio S, Acin A. Secure device independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2011(2): 238
- 28 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 2012, 108(13): 130503
- 29 Song T T, Wen Q Y, Guo F Z, *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. *Physical Review A*, 2012, 86(2): 022332
- 30 Ma X F, Fung C H, Razavi M. Statistical fluctuation analysis for measurement device independent quantum key distribution. *Physical Review A*, 2012, 86(5): 052305
- 31 Wang X B. Three-intensity decoy-state method for device-independent quantum key distribution with basis dependent errors. *Physical Review A*, 2013, 87(1): 012320
- 32 Ma X F, Razavi M. Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A*, 2012, 86(6): 062319
- 33 Silva F, Vitoreti D, Xavier G B, *et al.* Proof-of-principle demonstration of measurement device independent quantum key distribution using polarization qubits. *Physical Review A*, 2013, 88(5): 052303



- 34 Liu Y, Chen T Y, Wang L J, *et al.* Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 2013, 111(13): 130502
- 35 Li M, Zhang C M, Yin Z Q, *et al.* Measurement-device-independent quantum key distribution with modified coherent state. *Optics Letters*, 2014, 39(4): 880~883
- 36 Dong C, Zhao S H, Zhao W H. Measurement-device-independent quantum key distribution with odd coherent state. *Journal of Modern Optics*, 2014, 61(15): 1246~1250
- 37 Panayi C, Razavi M, Ma X F, *et al.* Memory-assisted measurement-device-independent quantum key distribution. *New Journal of Physics*, 2014, 16(4): 043005
- 38 Abruzzo S, Kampermann H, Bruss D. Measurement-device-independent quantum key distribution with quantum memories. *Physical Review A*, 2014, 89(1): 012301
- 39 Ma X C, Sun S H, Jiang M S, *et al.* Gaussian modulated coherent state measurement device independent quantum key distribution. *Physical Review A*, 2014, 89(4): 042335
- 40 Li Z Y, Zhang Y C, Xu F H, *et al.* Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 2014, 89(5): 052301



吴冰冰,女,博士,中国信息通信研究院通信标准研究所工程师,主要研究方向为高速光传输与光网络技术。

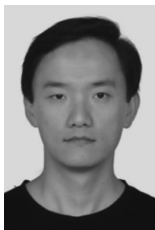


李少晖,男,博士,中国信息通信研究院通信标准研究所高级工程师,主要研究方向为高速光传输与光网络技术。



赵文玉,男,博士,中国信息通信研究院通信标准研究所高级工程师,主要研究方向为 40 Gbit/s/100 Gbit/s WDM、OTN 等光传送网新技术研究、标准制订以及系统测试评估。

[作者简介]



赖俊森,男,博士,中国信息通信研究院通信标准研究所工程师,主要研究方向为高速光传输与光网络技术。



张海懿,女,中国信息通信研究院通信标准研究所高级工程师、部门主任,主要研究方向为光传输系统、OTN、PTN、WDM 系统、SDH 系统、MSTP、自动交换光网络以及电信传送网络体制标准、运营商技术咨询。

2015142-7

2015 年 4 月份通信业经济运行情况

2015 年 4 月份,我国 3 家基础电信企业运行稳中趋缓,收入增长小幅回升。电信业务收入增速小幅回升。4 月,3 家基础电信企业电信业务总量完成 1 788.1 亿元,同比增长 22.6%,比上年同期增速高 6.8 个百分点;电信业务收入完成 976.9 亿元,按可比口径测算同比增长 3.6%,比上年同期及上月增速分别回落 2.3、0.9 个百分点。

2015 年 1-4 月,电信业务总量完成 6 887.5 亿元,同比增长 22.1%,继续保持加速增长趋势。电信业务收入完成 3 746.2 亿元,按可比口径测算同比增长 3.1%,比 1-3 月提高 0.2 个百分点,继续显现回升态势。4 月,4G 用户继续保持高速增长态势,净增超过 1 600 万户。光纤接入 FTTH/O 用户净增 357.3 万户,8 Mbit/s 及以上接入速率的宽带用户占比达 48.9%。

4G 移动电话用户月均净增超过 2 000 万户,移动宽带用户占比近 50%。1-4 月,移动电话用户净增 686.2 万户,不足上年同期的 1/3,移动用户数总规模达 12.93 亿户。移动电话用户结构继续优化,1-4 月,移动宽带(3G/4G)用户累计净增 6 172.3 万户,比上年同期净增数增长 7.6%,总数达到 6.44 亿户,在移动电话用户总数占比提升至 49.8%,较上年末提高 4.5 个百分点。其中,移动宽带用户的高速增长几乎全部由 4G 用户的发展带动,4 月净增 1 603.0 万户,总数达到 1.78 亿户,在移动电话用户占比 13.8%。

(来源:工业和信息化部运行监测协调局)