科学通报 2009 年 第 54 卷 第 16 期: 2277 ~ 2283
论 文 www.scichina.com csb.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

多层级量子密码城域网

许方星[①], 陈巍[①*], 王双[①], 银振强[①], 张阳[①], 刘云[①], 周政[①], 赵义博[①], 李宏伟[①②], 刘东[①], 韩正甫[①*], 郭光灿[①]

① 中国科学技术大学量子信息重点实验室, 合肥 230026;
② 中国人民解放军信息工程大学电子技术学院, 郑州 450004
* 联系人, E-mail: kooky@mail.ustc.edu.cn, zfhan@ustc.edu.cn

2009-06-23 收稿, 2009-07-16 接受
国家重点基础研究发展计划(编号: 2006CB921905)、国家自然科学基金重点项目(批准号: 60537020, 60621064)和中国科学院创新基金资助

摘要 由量子力学基本原理保证无条件安全的量子密码技术以及网络架构和应用模式研究是其实用化进程中的关键环节. 以“法拉第-迈克尔逊”量子密钥分配系统作为基础设备, 构造了一个多层级量子密码网络. 该网络应用了量子路由器、光开关和可信中继技术 3 种主流组网技术, 通过芜湖市电信商用光纤, 连接了包含 5 个政府部门在内的 7 个用户节点. 该网络可以满足电子政务所需的视频、音频、文字、文件等多种数据的量子保密传输, 向量子密码实际应用迈出了关键的一步.

关键词
量子密码
量子密钥分配
量子密码网络

最近20年, 随着实际量子密钥分配技术(quantum key distribution, QKD)的高速发展, 量子密码服务的应用也日趋成熟[1~5]. 量子密钥分配的安全性是由基本的物理原理所保证, 因此无论在公开信道中的窃听者如何攻击, 量子密钥分配系统都能够为用户提供具有无条件安全性的密钥[6,7]. 然而, 传统的点对点QKD协议在极限安全传输距离和用户的扩展方面均存在局限性. 虽然使用GHZ态或W态进行量子秘密共享可以使用户数多于两个[8~11], 但这种方法多用于量子传输而不适合实际的量子密码. 目前看来, 量子密码网络能够满足不断扩充的用户数需要和突发性的通讯要求, 并能与当前经典光网络适配, 是量子密码技术走向应用的必然需求.

自从Townsend等人[12,13]提出第一个使用光分束器搭建被动光网络(passive optical network, PON)来实现多节点量子密钥分配的想法之后, 人们提出了很多新的拓扑结构并在商用光纤线路上建成了实际量子密码网络. 第一个实际量子密码网络实验是由BBN公司在波士顿建成的, 通过主动切换光开关来控制一个三用户网络[14]. 随后, 我们在北京建成了四端口星型量子密码网络[15]. 在这种网络中使用了由波分复用(wavelength division multiplexing, WDM)器件构成的量子路由器, 可以实现自主路由分发. 2008年, SECOQC在维也纳建成的量子密码网络则是一个包含了5个用户和7条量子密钥分配链路[16]的网络结构. 最近, Chen等人[17]也实现了使用可信中继的三用户网络.

本文介绍了我们在芜湖市经典光通讯网上实现的全新多层级城域量子密码网络. 这个网络应用了量子路由器、光开关和可信中继等 3 种组网技术, 连接了城市中的 7 个节点, 组成了一个具有极高安全性的网络. 图 1 详细介绍了此量子密码网络的架构. 在这个网络中, 我们根据节点的优先级把它们分成多个层级. 一个高优先级的全通主干网连接了其中 4 个重要的节点, 每一个节点都可以当作一个子网网关来扩展网络结构. 另外的两个节点属于一个子网, 由一个光开关连接到主干网的节点 D. 第 7 个节点是通过一根单独光纤实现与量子密码网络的接入. 经

引用格式: 许方星, 陈巍, 王双, 等. 多层级量子密码城域网. 科学通报, 2009, 54: 2277~2283
Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991－2997, doi: 10.1007/s11434-009-0526-3

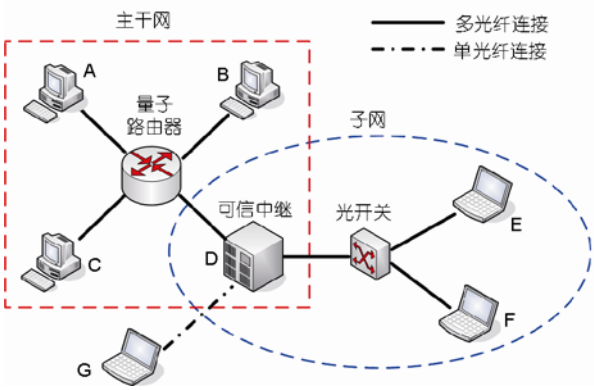

图 1 多层级量子密码网络结构示意图

网络中整合了量子路由器、光开关以及可信中继等 3 种组网技术. A~G 代表网络中 7 个不同的终端节点，分别归属于红色虚线方框中的主干网或是蓝色虚线圆圈中的子网. 图中的实线表示具有多根光纤的光学连接，而点划线代表单根光纤的光学连接

典信息交互和量子密钥分配都复用到同一根光纤中，展示了此量子密码网络在光纤资源匮乏的环境中也能很好地运转.

相比于以前的网络，这个量子密码网络第一次应用了多层级结构，并整合了 3 种不同的组网技术. 对于具有不同优先级和不同需求的节点，我们在网络设计中把它们分布在不同的层级上，并选用适当的网络连接技术，保证高效的网络效率. 所有的量子密钥分配连接都采用了结合诱骗态方案的 BB84 协议，保证通讯的安全性. 同时所有节点上运行的 QKD 程序以及用于加密声音图像以及文本的配套软件也已开发得较完善. 因此，这个量子密码网络不再是一个实验原型系统，而是一个面向用户的安全网络.

1 核心技术简介

1.1 基本量子密钥分配模块

网络中的每一条链路均由一对基本量子密码分配模块连接两个终端用户构成. 这里，我们使用了法拉第-迈克尔逊干涉环系统(FMI)来进行相位编码的量子密钥分配[3]. 由于普通单模光纤中偏振相关损耗(polarization dependent loss, PDL)和偏振模式色散(polarization mode dispersion, PMD)的影响，大部分实验室内QKD系统必须使用偏振控制器来稳定线路中偏振并减小其对系统的影响. 然而在实际的通讯机站里，这种器件对于已安装至标准机箱里的设备是不太方便的. 然而在FMI量子密码分配系统中，则不需要对偏振进行控制. 由于FMI结构中使用了法拉第镜，能极大地抑制线路中偏振的影响[7,18]. 单个法拉第镜的琼斯传输矩阵可以写成

$$FM = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \quad (1)$$

因此，信道的整体传输矩阵 T_{all} 可以表示为

$$T_{\mathrm{all}} = T^{-1} \cdot FM \cdot T = e^{i\varphi} FM, \quad (2)$$

其中T表征了单向的传输特性，可以看作是众多独立的双折射因素的总和. 前面的分析显示，无论光纤信道拥有怎样的双折射性质，输出光的偏振态总能保持与输入光的偏振态正交. 这种性质可以保证FMI量子密码分配系统能够自补偿信道偏振波动带来的影响. 在结合相位主动扫描技术后，能够在实际的光纤通讯线路中具有稳定的表现[3,5,19].

网络的通信资源也需要着重考虑. 在经典光网络中，出于成本考虑，只有需要高密钥生成率和低通讯阻塞的重要节点才会安装足够的光纤信道. 在非核心节点只有一至两根光纤引出并接到主干网上. 因此，我们设计了两种不同的方案来满足不同节点的需求. 方案一为如图 2 所示的原始 FMI 系统. 量子信号脉冲和同步信号脉冲具有相同的波长，在两根独立的光纤中传输. 另外，我们使用了商用的双向光端机来建立经典通讯连接. 这种光端机对通过互相发送 1550 nm 的强光脉冲，通信距离可以达到 30 dB 损耗(150 km 的标准单模光纤). 一般来说，它需要 4 根独立光纤. 其优点就是不会从其他的强光脉冲中引入串扰，保证了量子密码分配过程能够获得低的误码率(QBER)和高的密钥生成率. 这种方案的技术特点决定了它很适合用于通信资源充分的重要核心节点.

对于等级低、资源少的接入节点，我们则采用如图3所示的改进型方案. 相比于原始方案，4种不同的脉冲序列(经典通讯发送脉冲、经典通讯接受脉冲、量子信号脉冲和同步信号脉冲)通过一个环形器和一个波分复用器件(WDM)复用到一根光纤中，极大地节省在光网络中的光纤数目和通讯资源. 然而在这种方案中，拉曼散射和强光信号的串扰会显著地增加系统的误码率QBER，从而限制了系统的实际通讯能力[20]. 这种现象在下面的实际线路测试数据中也能反映出来.

1.2 架设主干网

作为网络的主体结构，主干网必须有足够的通讯能力将众多子网连接在一起. 因此，对于主干网需

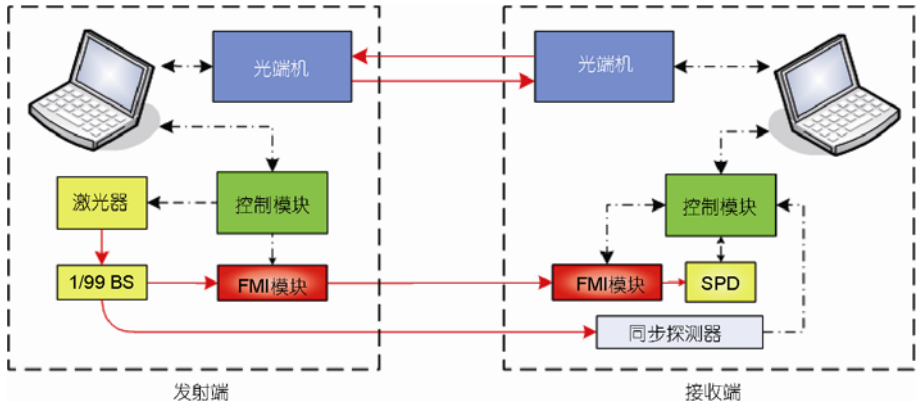

图 2　原始 FMI 量子密钥分配系统示意图

量子信号脉冲与同步信号脉冲产生于同一台激光器，经由一个 1:99 分束器(1/99 BS)后独立占用一根光纤. 加上经典通讯中光端机所需要的两根光纤，此系统共需要 4 根独立光纤，如图中红色实线所示. 点划线代表电学控制信号

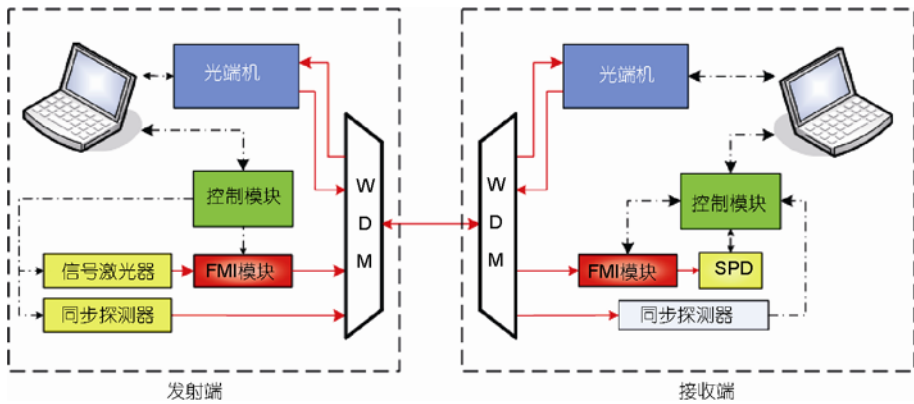

图 3　修改型的 FMI 量子密码分配系统

量子信号脉冲和同步信号脉冲使用了不同的波长. 每一个用户在进入公开信道的地方使用一个波分复用器件(WDM)对所有的输入和输出信号做复用和解复用，保证公开信道只需要一根光纤连接

要着重考虑的因素不再是高速的数据通过率，而是网络容量和信息阻塞率.

图 4 展示了用WDM器件搭建组成的量子路由器. 它能够实现自主路由寻址，即网络中两用户不需要任何主动地人工控制改变网络结构即可实现互通. 对于不同的通讯对象，用户只需要使用不同波长的光子即可. 一个由量子路由器连接而成的N端口网络，可同时建立$N(N-1)$条链路[21]. WDM器件固有的高隔离度也使得我们可以忽略信道之间的串扰而同时使用所有的信道[15]. 量子路由器的优点就是，不仅插入损耗小，而且不用进行经典通讯中可信中继常用的接收转发过程. 由于避免了这种会极大地延迟数据传输的操作，所以量子路由器很适合用于搭建多用户同时互通的主干网. 目前，使用现有商用器件搭建的这种网络结构可以引入多于 100 个核心用户，

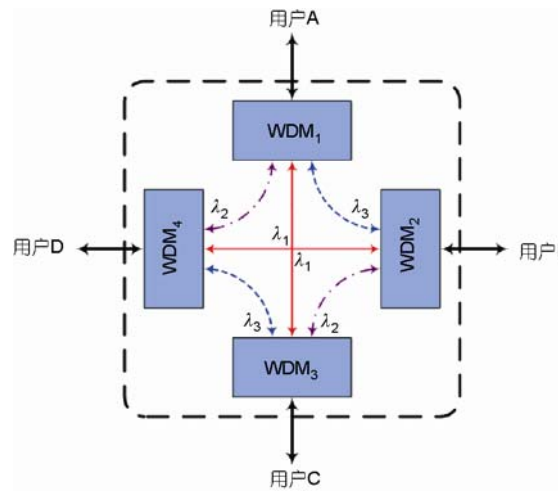

图 4　四端口量子路由器(quantum router, QR)结构示意图

用户 A 使用不同波长 λ_1, λ_2 和 λ_3 的光子分别与用户 B, C 以及 D 来连接. 量子路由器可以主动地将不同波长的光子路由到对应用户的输出端. 其他用户也利用相同的操作来建立 QKD 连接

更多的用户则可以通过扩展子网灵活地添加.

1.3 架设子网

子网的定义来自于经典通讯中的TCP/IP协议，是一个实际网络架构中的重要概念. 层级化的子网结构可以将整个网络分成很多高效的块结构，防止主干网络上的信息碰撞和阻塞. 对于一个子网，用户可以容忍一定的数据传输延时来获取更高的传输效率.

在图1的芜湖量子密码网络结构中，包含有一个典型的用光开关和可信中继搭建而成的子网部分. 节点D是主干网和子网的边界，作为一个可信中继网关控制子网与主干网之间的数据交互. 程控光开关则用于同步切换量子信号线路和同步信号线路来实现节点D到E的连接或者D到F的连接. 网络中的子网部分结构如图5所示.

光开关是一种简单易行的网络扩展方法[14,22]. 这种结构中，由于多条信道共用一部分链路，不仅会增加网络结构的复杂度，也会引起网络中的数据阻塞. 一旦网络中使用了大量的光开关，如何进行高效的信道远程控制和密钥管理将是非常重要的工作[23]. 可信中继则是经典通讯中常用的扩展通讯距离的方法[24,25]，其工作原理使得可信中继点对于途经的信息完全知晓. 只要可信中继是安全不被攻破的，那么量子密码网络的安全性就能得以保证. 同时，可信中继技术可以方便地应用于弱相干态QKD协议的诱骗态方案. 从目前的技术水平来看，可信中继是适合应用于大规模量子密码网络的技术.

1.4 网络协议

网络协议包含有两部分：一是在光网络中传输光子和分配量子密钥的协议，二是经典局域网(local area network, LAN)部分的通讯协议. 这两部分对于量子密钥分配过程和后续保密通信应用都非常重要，其中在经典局域网中，我们仍然使用最普及的TCP/IP协议，使得所有的通讯交互模块都以此协议连接，也方便此量子密码网络与更大范围的以太网或因特网相结合. 在芜湖量子密码网络中，由于网络机站和机房中都无法提供以太网接口，我们根据1.1节中描述的系统方案，使用光端机架设了局域网来进行经典通讯.

对于量子密钥分配过程，网络中所有的链路均采用了相位调制BB84协议的诱骗态方案. 在诱骗态方案中，诱骗态脉冲随机地参杂在信号态脉冲序列中. 由于我们假设窃听者无法区分截获的光子是来自于诱骗态脉冲还是信号态脉冲，那么信号态的传输效率和误码就可以通过诱骗态的测量结果来进行估计[26~29]. 根据文献[30](即GLLP)，最终的密钥生成率可以用下式计算:

$$R \geqslant q\{-Q_\mu f(E_\mu)H_2(E_\mu)+Q_1^{L,\nu,0}[1-H_2(e_1^{U,\nu,0})]\}, \quad (3)$$

其中q是FMI方案的传输效率，$f(e)=1.2$是双向纠错算法的效率，$H_2(x)=-x\log_2 x-(1-x)\log_2(1-x)$是二维熵函数. Q_μ, E_μ表示平均光子数为μ的信号态的计数率和误码率. Q_1和e_1则是单光子态的计数率和误码率，其边界值可以估计为[31]

$$Q_1 \geqslant Q_1^{L,\nu,0}=\frac{\mu^2 e^{-\mu}}{\mu\nu-\nu^2}\left(Q_\nu e^\nu-Q_\mu e^\mu\frac{\nu^2}{\mu^2}-\frac{\mu^2-\nu^2}{\mu^2}Q_{vac}\right), \quad (4)$$

$$e_1 \leqslant e_1^{U,\nu,0}=\frac{\mu e^{-\mu}}{\mu-\nu}\frac{E_\mu Q_\mu e^\mu-E_\nu Q_\nu e^\nu}{Q_1^{L,\nu,0}}. \quad (5)$$

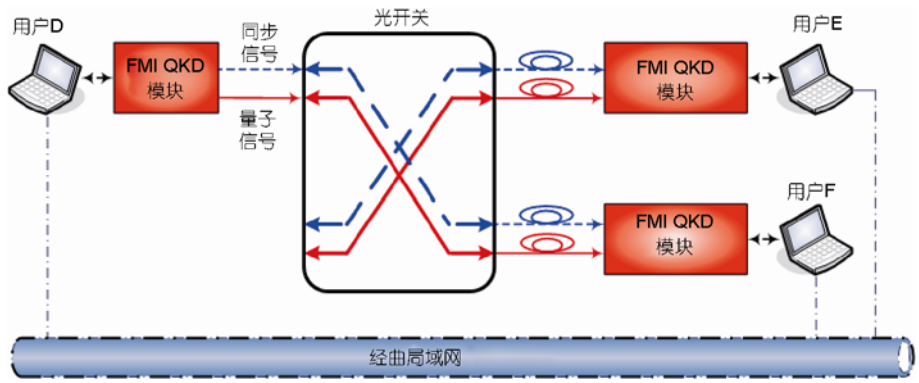

图 5 包含三用户的光开关子网结构示意图

用户之间量子信道和同步信道由光开关阵列同时切换，保证不同链路的畅通. 实际系统中已预先用光端收发机为子网中的用户搭建好经典的局域网(LAN)

在考虑了测量的统计涨落后，上式中的 Q_v 和 Q_{vac} 应该用它们的上限或者下限来代替，即

$$Q_x^{L}=Q_x\left(1-\frac{10}{\sqrt{N_xQ_x}}\right), \tag{6}$$

$$Q_x^{U}=Q_x\left(1+\frac{10}{\sqrt{N_xQ_x}}\right), \tag{7}$$

其中 $x=\mu, v, vac$ 分别代表信号态、诱骗态和真空态，N_x 则为 3 种脉冲各自的脉冲数目. 在 20 min 的现场测试中，样本数目 N_x 为 10^9，Q_x 的上下限波动小于 $0(10^{-2})Q_x$，因此我们可以忽略统计涨落而直接使用计数率的测量值. 另外，虽然用于产生诱骗态和真空态的光强调制器的消光比最大能达到 25 dB，但这里所说的真空态并不是真正的真空态. 所以在估算 e_1 的上限时，更准确的估算方法应该是使用诱骗态的计数率和误码率 Q_v 和 E_v，而不是使用 Q_{vac}.

根据在量子密码城域网中测量的数据，我们可以利用上述公式估算出最终的密钥生成率，并根据它来进行 CASCADE 纠错和用二维 Hash 函数来做保密放大. 经过了这些后续处理后，两终端用户就能共享一串安全的密钥，用于实际保密通讯应用.

2 现场测试

图 6 是整个量子密码网络的分布卫星图，各个节点分布在芜湖市的光通信网上. 相比于实验室环境中的实验系统，在这样一个实际的通讯网中，突发性的外界振动影响和来自于经典光网络中强光信号的干扰对量子密钥分配系统的稳定性和鲁棒性都是严峻的考验. 然而测试数据结果清楚地显示了芜湖量子密码网络是可以在这种条件下实际应用的.

我们让整个网络在实际现场连续不停地运行来检验其性能. 所有的量子密码分配系统频率设置在 5 MHz，系统中的两种性能相近的单光子探测器，包括

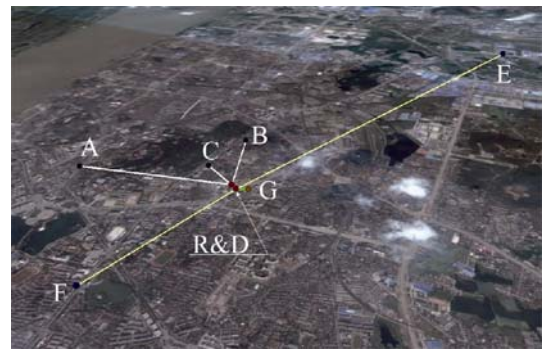

图 6 坐落在安徽省芜湖市的量子密码网络中各节点的卫星分布图

节点 A 是芜湖市科技局，节点 B 是芜湖市经济委员会，节点 C 安置在芜湖市总工会. R 代表量子路由器，和节点 D 一起，安置在电信机房中. 这 4 个节点构成了网络中的主干网部分. E 和 F 安置在质量监督局和招商局内，他们由光开关连接成一个子网. 节点 G 在电信机房内，通过一根 500 m 的光线接入到网络中，来检验单根光纤接入的量子密码分配系统方案

id200 单光子探测器(idQuantic公司)和自制的单光子探测器，量子探测效率为 10%，暗计数大致在 1×10^{-6} 量级. 经过主动相位补偿之后，干涉条纹可见度平均稳定在 98.67%. 结合法拉第-迈克尔逊干涉环结构和单光子探测器产生的固有误码率，对全部链路我们把诱骗态方案中信号光平均光子数设成 $\mu=0.6$，而把诱骗态的光强设成 $v=0.2$[31]. 3 种不同的脉冲数比率定为 6:3:1. 以这些参数设定进行的量子密码分配过程，可以使链路两端产生有误码的密钥串. 经过CASCADE纠错和Hash函数做保密放大，即可保证双方共享一致的无信息泄露的密钥.

表 1 列出了此网络中所有 9 条链路的具体参数和最终密钥生成率. 网络版附录中的表 2 则给出了详细的网络现场测试数据. 各条链路的光纤长度和线路损耗都已列出，其中节点 D 和 E 之间距离最远可以达到 10 km，但是节点 A 和 C 之间的链路却有最大的衰

表 1 量子密码网络全部链路的参数和密钥生成率 a)

Route	A-R-B	A-R-C	A-R-D	B-R-C	B-R-D	C-R-D	D-S-E	D-S-F	D-G
Wavelength/nm	1550	1530	1510	1510	1530	1550	1530	1530	1510
Distance/km	5.0	5.6	3.5	3.6	1.5	2.1	10.0	5.0	0.5
Attenuation/dB	6.28	7.18	4.42	5.13	2.39	4.37	6.23	6.14	1.0
Sifted key/kbps	3.38	2.56	5.32	4.36	8.25	5.42	3.15	3.27	11.0
QBER	2.19%	1.87%	1.96%	2.15%	1.93%	1.8%	2.34%	1.89%	3.8%
Final key /kbps	0.74	0.61	1.73	0.82	2.53	1.58	0.49	0.66	0.08

a) “Route”代表每一条链路的具体路径，其中 A~G 代表 7 个不同的节点，R 是量子路由器，S 是程控光开关矩阵. “Distance”是链路光缆的实际长度，由于接入损耗和其他因素，它并不能保证与实际信道衰减成正比

减, 为 7.18 dB. 这也说明了在实际光纤线路中, 除了光纤每公里 0.2 dB 的衰减, 连接的插入损耗同样是损耗的主要来源. A~F 这 6 个节点分别通过量子路由器或者光开关阵列连接到整个网络中, 它们之间均采用原始的 FMI 量子密钥分配方案, 系统传输量子信号态的误码率在这样的 10 km 城域范围内能够稳定在 1.8%~2.4%, 据此就能计算出对基后的原钥率和最终密钥率. 对于不同的线路衰减, 最终密钥生成率在 2.5 kbps 到 0.5 kbps 变化. 最后一个接入节点 G 到 D 的连接, 则是采用了修改型的 FMI 系统方案, 只使用一根 500 m 的光纤连接到主干网上, 线路损耗约为 1 dB. 由于线路的经典信号的串扰和拉曼散射, 误码率 QBER 显著增长到 3.8%. 其结果就是, 虽然对基后的原钥率有 11 kbps, 但经过后处理后的最终净密钥率只有 83 bps. 这也反映了对于量子密码分配过程, 原钥率和误码率都会对最终密钥率产生很大的影响. 前者主要取决于系统的效率和工作速度, 以及网络中的链路路由技术等; 而后者则主要由干涉环系统的平衡性和单光子探测器的性能来决定. 为了在将来能获得更高的密钥生成率, 我们将着重关注高速量子密钥分配系统的研究以及更好性能单光子探测器的开发.

以现有的量子密码分配系统, 其密钥生成率是不足以进行一次一密算法应用的, 特别是对于实时的动态图像这种数据量巨大的流媒体而言. 因此, 我们把量子密码分配产生的密钥作为 AES(advanced encryption standard)算法的 128 位密钥来加密明文, 并进行快速更新. 以此为基础, 我们在密码网络上的各单位之间进行了一个实际的量子网络会议. 我们可以把视频和声音信息经过 AES 加密后的密文在自架设的局域网中发送给特定的用户, 并在接收端进行解密, 实现安全的实时信息传输. 同时, 实时的短消息和保密文件也可以通过配套量子密码分配的软件实行相同过程的安全通讯, 满足了电子政务所需的多种数据的量子保密传输.

3 结论

2009年5月, 我们在芜湖市建成了具有多层级结构的7用户量子密码网络. 这个量子密码网络以“法拉第-迈克尔逊”干涉环结构为基础模块, 能够在实际光纤线路上保持长时稳定的密钥分配. 为了获得高效的网络通讯效率, 整个网络被分成了优先级不同的两个部分: 一部分是以量子路由器连接而成的全时全通主干网, 用来保证高网络容量和低信息阻塞率, 另一部分是基于光开关和可信中继技术的子网, 用来保证量子密码网络的灵活性和扩展性. 网络中分发的安全密钥, 可以用于实现用户之间实时的视频、声音、实时短消息以及保密文件等各种数据的保密传输. 整个网络应用包含有完整的量子密钥分配过程和配套的应用程序软件, 是一个真正面向用户、具有无条件安全性的实际保密网络.

致谢 感谢芜湖政府和中国电信集团芜湖分公司的支持.

参考文献

1 Muller A, Herzog T, Huttner B, et al. “Plug and play” systems for quantum cryptography. Appl Phys Lett, 1997, 70: 793—795[DOI]
2 Gobby C, Yuan Z L, Shields A J. Quantum key distribution over 122 km of standard telecom fiber. Appl Phys Lett, 2004, 84: 3762—3764[DOI]
3 Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Opt Lett, 2005, 30: 2632—2634[DOI]
4 Zhao Y, Qi B, Ma X F, et al. Experimental quantum key distribution with decoy states. Phys Rev Lett, 2006, 96: 070502[DOI]
5 Takesue H, Nam S W, Zhang Q, et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nat Photonics, 2007, 1: 343—348[DOI]
6 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984. 175—179
7 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145—195[DOI]
8 Zeng G H, Keitel C H. Arbitrated quantum-signature scheme. Phys Rev A, 2002, 65: 042312[DOI]
9 Chen K, Lo H K. Multi-partite quantum cryptographic protocols with noisy GHZ states. Quant Inform Comput, 2007, 7: 689—715
10 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret sharing schemes. Phys Rev A, 2004, 69: 052307[DOI]

11 闫凤利, 高亭, 李有成. 用 4 个量子态实现的多方与多方之间的量子秘密共享. 中国科学 G 辑: 物理学 力学 天文学, 2008, 38: 241—249

12 Townsend P D, Phoenix S J D, Blow K J, et al. Quantum cryptography for multi-user passive optical networks. Electron Lett, 1994, 30: 1875[DOI]

13 Townsend P D. Quantum cryptography on multi-user optical fibre networks. Nature, 1997, 385: 47—49[DOI]

14 Elliott C. Building the quantum network. New J Phys, 2002, 4: 46[DOI]

15 Chen W, Han Z F, Zhang T, et al. Field experimental "star type" metropolitan quantum key distribution network. IEEE Photonics Tech Lett, 2009, 21: 575—577[DOI]

16 Poppe A, Peev M, Maurhart O. Outline of the SECOQC quantum-key-distribution network in Vienna. Int J Quantum Inf, 2008, 6: 209—218[DOI]

17 Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography. Optics Express, 2009, 17: 6540—6549[DOI]

18 Han Z F, Mo X F, Gui Y Z, et al. Stability of phase-modulated quantum key distribution systems. Appl Phys Lett, 2005, 86: 221103[DOI]

19 陈巍, 韩正甫, 莫小范, 等. 量子密钥传输系统的主动相位补偿. 科学通报, 2007, 52: 2221—2225

20 Subacius D, Zavriyev A, Trifonov A. Backscattering limitation for fiber-optic quantum key distribution systems. Appl Phys Lett, 2005, 86: 011103[DOI]

21 Zhang T, Mo X F, Han Z F, et al. Extensible router for a quantum key distribution network. Phys Lett A, 2008, 372: 3957—3962[DOI]

22 Tang X, Ma L J, Mink A, et al. Demonstration of an active quantum key distribution network. Proc SPIE, 2006, 6305: 630506[DOI]

23 Wen H, Han Z F, Guo G C, et al. The queuing model for quantum key distribution network. Chin Phys B, 2009, 18: 46—50[DOI]

24 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chinese Sci Bull, 2009, 54: 158—162[DOI]

25 Wen H, Han Z F, Zhao Y B, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. Sci China Ser F, 2009, 52: 18—22[DOI]

26 Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901[DOI]

27 Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett, 2005, 94: 230503[DOI]

28 Lo H K, Ma X F, Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504[DOI]

29 Wang X B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. Phys Rev A, 2005, 72: 012322[DOI]

30 Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices. Quant Inform Comput, 2004, 5: 325—360

31 Ma X F, Qi B, Zhao Y, et al. Practical decoy state for quantum key distribution. Phys Rev A, 2005, 72: 012326[DOI]

附录 现场实验数据

表 2 量子密码网络现场测试数据 [a)]

Route	A-R-B	A-R-C	A-R-D	B-R-C	B-R-D	C-R-D	D-S-E	D-S-F	D-G
N_{μ}	1.25×10^{9}	1.40×10^{9}	1.08×10^{9}	1.23×10^{9}	1.11×10^{9}	1.23×10^{9}	1.18×10^{9}	1.08×10^{9}	1.20×10^{9}
Q_{μ}	0.0069169	0.0052029	0.0108466	0.0085879	0.0167524	0.0106854	0.0063737	0.0065981	0.022125
E_{μ}	0.0219	0.0187	0.0196	0.0215	0.0193	0.0180	0.0235	0.0189	0.0380
N_{v}	6.27×10^{8}	7.00×10^{8}	5.40×10^{8}	6.14×10^{8}	5.53×10^{8}	6.14×10^{8}	5.90×10^{8}	5.41×10^{8}	6.02×10^{8}
Q_{v}	0.0024508	0.0018022	0.0040541	0.0029451	0.0061579	0.0038264	0.0021723	0.0022359	0.007593
E_{v}	0.0307	0.0312	0.0331	0.0309	0.0326	0.0330	0.0306	0.0278	0.0425
N_{vac}	2.09×10^{8}	2.33×10^{8}	1.80×10^{8}	2.05×10^{8}	1.84×10^{8}	2.05×10^{8}	2.05×10^{8}	1.80×10^{8}	2.01×10^{8}
Q_{vac}	0.0001074	0.00009	0.0001233	0.0001539	0.0002112	0.0001586	0.0001180	0.0001319	0.000396
E_{vac}	0.2016	0.1564	0.2323	0.1485	0.1994	0.1947	0.1575	0.1511	0.1588
时间	1283 s	1426 s	1103 s	1214 s	1125 s	1213 s	1196 s	1094 s	1212 s

a) “Route”代表每一条链路的连接路径. N_X, Q_X, E_X 则分别为 X 态脉冲数目、计数率以及误码率, 其中 $X=\mu, v, vac$ 分别对应信号态脉冲、诱骗态脉冲以及真空态脉冲. 所有的数据来自于长时间运行过程中的 20 min 测量过程